Software Security and Privacy Risks in Mobile e-Commerce

Article Review by David Oluwamayowa Fakunle
Email: davidfakunle@gmail.com

Source

Ghosh A K, Swaminatha T. M, 2001, 'Software Security and Privacy Risk in Mobile E-commerce', Communications of the ACM, February, Vol. 44, No. 2, pp. 51-7, viewed 27 January 2015, https://www.cs.indiana.edu/~shiny/oral_qual/files/p51-ghosh.pdf.

Introduction

This review will analyse the article 'Software Security and Privacy Risk in Mobile E-commerce' in the online journal of Communications of the ACM. This review will first summarise the article. Secondly, it will look at the effectiveness of the article's structure, the arrangement of the information and reader ease of access.Thirdly, the review will critique the article, authority, accuracy, currency, objectivity and its relevance. The review will analyse the strategy presented by the author. The article was useful, clear and important

Review of Literature

Top security experts have written on this topic highlighting the need for application designers to consider user security while building and executing their applications. Mobile electronic commerce which is fast becoming the most convenient approach by users to transact their business without having to engage face to face with business owners are prone to the activities of cyber hackers. Recent publication have focused on encouraging a common platform that application designers will build on irrespective of the devices used and provide the necessary security intelligence to protect the users as they will feel more comfortable entering their personal data on their own wireless devices.

Article Summary

The purpose of the article is to provide the relevant principal areas to be considered to enable mobile e-commerce thrive. Owing to the vast prospects the sector will provide and the future of business transactions, it is imperative for the policy makers to understand the risks posed by wireless devices while accessing e-commerce applications. With the success recorded in desktop e-commerce system and the ability to reduce malicious attacks on e-commerce systems, the article highlighted the need for operators to use a common interface and build on strengthening it to ensure data security and reverence for privacy even as customers move from desktop e-commerce systems to mobile e-commerce systems. Mobile e-commerce systems will introduce new security and privacy risks beyond those currently found in desktop e-commerce systems. Encrypted communication protocols are necessary to provide confidentiality, integrity and authentication for mobile e-commerce applications.

Article Structure

The article in its introduction opened with expectations of wireless, internet enabled devices and how it perceived to be accepted by users for future business communication. The paragraphs in the body were short and concise containing 6 body heading with in depth information explaining the acts and mode of operation. As the article defined the research study conducted by the authors, the article contained real time strategies that will help to inform the reader. The authors highlighted the growth of the e-commerce business and how companies can leverage on the emerging market opportunities through limiting security flaws and privacy concerns for mobile users to carry out daily transaction with the assurance of the same even improved security enjoyed via the desktop.

The findings were explicit even in details and provided a fora for technology collaboration. The conclusion was short and contained the submission of the authors towards implementation of the standard best practices for continuous existence of business operations. References were identified with numbers which was easy to access. The article was logically developed, jargons were professionally explained which makes it easier for non-technical personnel understand the authors point of view. The article was presented in a PDF format preserving the formatting. Though no internal link in the body of the article, the authors were able to crystallize their opinions accurately.

Article critique

Authority

The journal, Communication of the ACM is the leading print and online publication for computing and information technology fields. Over 100,000 ACM members have access to its print magazine with in-depth coverage of emerging areas of computer science, new trends in information technology and practical applications. They have been providing platform to present and debate various technology implications, public policies, engineering challenges and market trends for over 50 years.

The authors are Information Technology Security Experts. Mr. Ghosh is Director of Security Research while Mr. Swaminatha is the software Security consultant both at Cigital Inc.at the time this article was published.

Accuracy

The source of the information in this article is fairly recent. It was supported with prevalent, recent reference list with these sources cited in text to support the research. The reporting and decisive processes contributed to the article's accuracy.

Currency

The journal was published in February 2001. The research it describes was current and the article cites up to date references in the body of the text (ranging from 1998-2000). Therefore, the article is current as at time of publication.

Relevance

This article on the ACM database and accessed by over 100,000 members worldwide will provide insight into current trends for Information Technology professionals. It would be relevant to key stakeholders interested in exploring the opportunities mobile e-commerce will offer. It could be difficult for entry level professionals not familiar with security and privacy risks for wireless internet enabled devices.

Objectivity

The information was factually presented. The article acknowledged that users of wireless devices can be difficult to trace because wireless devices roam in and out of wireless zones, having no fixed geographical point, and can go online and offline easily. Furthermore, without foundational security model, the severity of attacks against wireless devices will increase as these devices become more critical to users and businesses for both storage and processing of confidential information.

Stability

The article with its source on ACM database is stable as a resource and serve to inform technology leaders.

Analysis of graph/Image/Table

(Not Applicable)

Recent Advances Related to the Topic

Some of the recent advances on mobile ecommerce security includes fraud detection, application security, infrastructure protection, identity and access management as well as security intelligence and analytics. E-commerce applications overtime in its bid to earn the trust of users have implemented these security capabilities into their applications.

Conclusion

Mobile commerce itself present new risks, the nature of the medium requires a degree of trust and cooperation between nodes in networks that can be exploited by malicious entities to deny service and as well collect confidential information and disseminate false information. The best strategy for addressing security and privacy risks of internet-based content is to build security into the platform and applications themselves rather than attempt to introduce security patches afterward.

Reference

[1.] Arehart, C. and et al. *Professional WAP*. 1st edition, Wrox Press, 2000.

[2.] Balfanz, D. and Felten, E. Handheld computers can be better smartcards. In *Proceedings of the Eighth USENIX Security Symposium*,USENIX Association. (Aug. 1999, Washington, DC).

[3.] Cowan, C. et al. Buffer overflows: Attacks and defences for the vulnerability of the decade. In *Proceedings of the DARPA Information Survivability*

[4.] *Conference and Exposition (DISCEX 2000)*, (Jan. 2000, HiltonHead, SC), IEEE Computer Society, Los Alamitos, CA.

[5.] Cranor, L. F. Internet privacy: A public concern. *netWorker 2*, 3(June/July 1998), 13–18; www.acm.org/pubs/citations/journals/networker/1998-2-3/p13-cranor/.

[6.] Ghosh, A. K. *Security and Privacy for E-Business.* Wiley, NY (Jan. 2001).

[7.] Haskin, D. Analysts: Smart phones to lead e-commerce explosion. *all-Net Devices*(Nov. 3, 1999); www.allnetdevices.com/news/9911/991103ecomm/ 991103ecomm.html.

[8.] Lewis, T. Ubinet: The ubiquitous Internet will be wireless. *IEEE Computer32*, 10 (Oct. 1999).

[9.] Strategy Analytics. Strategy Analytics forecasts $200 billion mobilecommerce market by 2004. Wow.com, January 10, 2000; www.wowcom.com/newsline/press_release.cfm?press_id=862.

[10.] WAP Forum. Technical Reports WAP-193-WMLScript, WAP-170-WTAI, WAP-169-WTA. June–July 2000; www.wapforum.org.

[11.] Zhang, Y. and Lee, W. Intrusion detection in wireless ad-hoc networks.In *Proceedings of the ACM/IEEE MobiCom*, (Aug. 2000).