View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by The International Islamic University Malaysia Repository

Online Authentication Using Smart Card Technology in Mobile Phone Infrastructure

Teddy Mantoro, International Islamic University Malaysia, Malaysia

Admir Milišić, International Islamic University Malaysia, Malaysia

Media A. Ayu, International Islamic University Malaysia, Malaysia

ABSTRACT

The widespread of Internet usage has resulted in a greater number and variety of applications involving different types of private information. In order to diminish privacy concerns and strengthen user trust, security improvements in terms of authentication are necessary. The solutions need to be convenient, entailing ease of use and higher mobility. The suggested approach is to make use of the already popular mobile phone and to involve the mobile network, benefiting from Subscriber Identity Module (SIM) card's tamper resistance to become trusted entities guarding personal information and identifying users. Mobile phone's SIM card is convenient for safely storing security parameters essential for secured communication. It becomes secure entity compulsory for getting access to privacy sensitive Internet applications, like those involving money transfers. Utilizing the NFC interface passes the personal user keys only when needed, giving additional strength to the traditional public key cryptography approach in terms of security and portability.

Keywords: *Mobile Phone, Near Field Communication, Online Authentication, Public Key Cryptography, SIM Card, Smart Card*

INTRODUCTION

Perhaps due to the lack of experience and knowledge among most of the Internet users, combined with unsatisfying security level regarding online software and websites, the Internet user privacy becomes more of an issue each year. As numbers are constantly increasing in terms of services available, connected users and networked devices, Internet community is faced with inherited, new risks that need to be dealt with. Firstly, due to the rise of social networking sites, most notably Facebook, typical user names are becoming less common and real data is used instead. Now ramifications of compromised accounts are more serious and could possibly lead to identity theft. Recent case of personal data leakage involving Facebook, when private details of 100 million users were exposed, illustrates the gravity of situation (Hough, 2010). Secondly, the proliferation of the Internet has given rise

DOI: 10.4018/jmcmc.2011100105

Copyright © 2011, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

to electronic commerce or e-commerce, based on buying and selling online. Because the trust is essential for successful business transactions, the difficulties in protecting information confidentiality and integrity have the greatest impact on e-commerce development. The problem is significant decrease of confidence in online payment system when there is even the slightest possibility or mere rumor of potential flaws in terms of security or convenience. Most of the users still have concerns about the privacy when dealing with "faceless" e-commerce web sites. Similarly, some users are more cautious and more reluctant to adopt new trends, like social networking web sites, due to the fears of their personal information being unrightfully exposed. Even though most of the people are reckless unless material well being (i.e., the money) is involved, in time, as the dangers of stolen private information become apparent, service providers in general will definitely be compelled to do more in order to reassure customers and keep their trust.

Computers could be compared to buildings, due to the fact that both keep some objects and, more or less, guard them against intruders and limit the access to those who are authorized. Considering the buildings, most of them have doors and locks, which is the basic security measure. However, throughout history, with new technologies and ideas, new mechanisms were invented and then used in combination with common locks. These new, different mechanisms are normally not considered as a replacement to one another, but rather an additional security layer to be used together with what was already there. So today, breaking into a museum and retrieving a valuable artifact is not an easy task and requires highly skilled team of diverse expertise and skills. In addition to locked doors there are guards, security cameras, lasers and bulletproof glass boxes that need to be faced.

The reason some buildings have more security layers than others, is because they host objects which are of greater value. In the same way, as the Internet applications become more diverse and more complex, the value of user account relevant information becomes higher and of greater importance. Therefore, with increasing number of applications handling private information, the time has come to consider another layer for user authentication, in addition to common method of user name and password combination. The chances of assuming other person's identity or tampering with their account information would be smaller that way, since more resources would be required on attacker's side in terms of money, skill and work force. Furthermore, the users of various Internet services would be reassured and thus feel more confident to entrust their private information to the providers. However, there is additional factor that needs to be kept in mind while devising a solution. No matter how effective authentication method may be, the success of it also depends on user convenience which entails ease of use and mobility.

There are three general methods to validate user's identity: something they know (username and password), something they have (smart card) and something about them (biometrics) (Stamp, 2006). In addition to common username and password login, the proposed solution is the involvement of mobile phone hosting SIM (Subscriber Identity Module) card with additional functionality of securely storing critical information related to the client side computer application. Among things that smart card (i.e., SIM) stores could be keywords that acknowledge user's identity or cryptography keys that can be employed to secure the communication channels. These parameters can be combined as well or supplemented with additional ones if developers find them necessary and see it as an improvement. The key point and foundational idea is the combination of smart card's security-wise robustness (it cannot be accessed without appropriate driver and authorized reader) and convenience of using familiar and common mobile phone in the secured Internet authentication and communication. This provides more efficient protection against Trojans and malicious individuals that seek to deceive and exploit. Computer application, or certain parts of it (those dealing with money transfer, for

Copyright © 2011, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

15 more pages are available in the full version of this document, which may be purchased using the "Purchase" button on the product's webpage:
www.igi-global.com/article/online-authentication-using-smart-card/58906

Related Content

Building an Intelligent Mobile Advertising System
Jerry Zeyu Gao and Angela Ji (2010). *International Journal of Mobile Computing and Multimedia Communications (pp. 40-67).*
www.igi-global.com/article/building-intelligent-mobile-advertising-system/40980

Cooperative Caching in Mobile Ad Hoc Networks
Naveen Chauhan, Lalit K. Awasthi, Narottam Chand, R.C. Joshi and Manoj Misra (2011). *International Journal of Mobile Computing and Multimedia Communications (pp. 20-35).*
www.igi-global.com/article/cooperative-caching-mobile-hoc-networks/55865

Mobile Business Process Reengineering: How to Measure the Input of Mobile Applications to Business Processes in European Hospitals
Dieter Hertweck and Asarnusch Rashid (2009). *Mobile Computing: Concepts, Methodologies, Tools, and Applications (pp. 2391-2417).*
www.igi-global.com/chapter/mobile-business-process-reengineering/26670

Channel Choices and Revenue Logics of Software Companies Developing Mobile Games
Risto Rajala, Matti Rossi, Virpi Kristiina Tuunainen and Janne Vihinen (2009). *Mobile Computing: Concepts, Methodologies, Tools, and Applications (pp. 2463-2474).*
www.igi-global.com/chapter/channel-choices-revenue-logics-software/26673