The evolution of technology

Technology, Mobile Phone

The evolution of technology over the past few years has been part of a phenomenal experience in our everyday lives. Today, more and more people rely on getting things done faster and quicker, with the help of technology. Take banking for instance, the traditional way was having to go to the bank for even the smallest transactions like sending money, checking your balance and so on. Then came the era of Automatic Teller Machines (ATMs), which can be used to carry out simple banking transactions. From then on, Internet banking was introduced in the early 1980s, and by the year 2000, around 13. 7% of households had signed up for online banking accounts, just in America (Ann Lomena, Joy Ried, Dec 2000).

Today the new innovation in the banking sector is all about Mobile Banking. With the rapid increase in mobile applications development, as well the increase in use of ‘ smart phones’, more and more people are comfortable with viewing their account balance information and transactions history on their mobile phones. According to Celent, 2007, 73% of consumers would want to use their mobile phones to view their bank account details.

As good as Mobile Banking sounds in terms of getting faster and easier access to banking services from any location, the idea of mobile banking also brings along some security issues regarding safe transmission of information. Just like the old saying that goes, “ every coin has two sides”, mobile banking also has its disadvantages despite how excellent and convenient the technology might seem to be.

Pros and Cons of Mobile Banking

The most popular mobile banking services provided by major banks include: account alerts and reminders, account balances, updates and history, customer service, information on locations of ATMs or branches of the bank and bill payments; for instance people can now pay their utility bills like water and electricity bills via a mobile phone. Safaricom and Zain mobile companies in Kenya also provide a service by which subscribers can send money from one organization or individual to another. This makes it easier and expedient for users to pay their bills, or send money across to other accounts. Most of the banking in this case is carried out via the SMS service, which is good and reliable, however not very secure.

Other services are provided via a bank's WAP site, which is rendered on a mobile phone, through which a user can access his account. The advantages of using a WAP site for mobile banking are easy-to-use and understandable user interfaces, and often offer a secure connection between the mobile handset and the banking website. On the other hand, these services may only be available and in working condition on particular types of handsets only, and sometimes they may only be accessible on some mobile browsers and not others.

Based on the arguments stated above, Mobile Banking is proven to be more economical and convenient to both the banks as well as its consumers; however it is also significant to look at some of the security threats that this technology comes along with.

Potential Security Threats Related to Mobile Banking

The most well-known security breach known today is phishing. Many of the huge multinational IT Security organizations are fighting to deal with this problem, but there always seems to be a loophole somewhere in the systems that hackers identify and get into. Phishing can be defined as the act of tricking users into disclosing personal and sensitive information (Mobile Banking Overview, Mobile Marketing Association, Jan 2009).

Another threat is the existence of Malware, which is malicious code that can be downloaded unintentionally onto the mobile phone as a worm or a virus. These kinds of codes are used to collect personal data like names, addresses, passwords, and this case, bank account details. Hijacking is also a risk to be considered when talking about mobile banking, and also internet banking, for this matter. This is a situation in which the hacker or hijacker will impersonate either the banking society or the consumer. Users can think they are communicating with the bank officials, while in reality they may be broadcasting their personal information to wrong parties. Hackers can take advantage of such confidential information and succeed in their fraudulent actions such as making unauthorized transactions in their favor.

Third party mobile applications can also play a role in collecting confidential information for wrong intended purposes. In order to carry out some banking transactions, users may be advised to download particular applications, but as far as internet fraud goes, the user may accidentally download a third party application, thinking that the software is controlled by the bank. This can be dangerous as the financial information regarding the user’s bank account will be compromised and in the hands of deceitful people.

Security flaws in the Mobile Banking Applications could also result as a threat to the user. Most of these banking applications make use of Global System for Mobile Communications (GSM) technologies and General Packet Radio Service (GPRS) technologies (Prof. T. A. Gonsalves, March 2008). Based on my past experience in the IT field, I can imply that the security of a banking transaction being carried out on a mobile phone depends on the security of data transfer through the various modes of communication, in this case being GSM and GPRS.

Are Mobile Banking Technologies Secured?

GSM provides a security measure for authorized access. Each SIM card used has to be certified before it can get access to any GSM network. If authentication fails at this stage, then no access is provided to the network and the SIM card fails. However, this cannot be categorized as a guaranteed secure environment as the authentication algorithm has once been outwitted by Wagner and Goldberg (Wagner, D. GSM Cloning. Smartcard Developer Association, 1998).

GPRS is used to connect to WAP (Wireless Application Protocol) sites on the mobile phones. The loopholes with this technology are concerned with sending encrypted information across from one point to another. When Information is in encrypted form, it is not understandable by any users or third parties. This is great, because it can ensure a secure path for data transmission, although the problem with this technology is that the encryption is not end-to-end, from the client’s mobile phone, straight to the servers at the bank. There is a gateway in-between from where the information passes, and chances are that malicious software or hackers can break into the transmission at the gateway, and steal confidential data.

What can be done to improve Mobile Banking Security?

One solution is to redefine the protocols used in telecommunications. Enhancing protocols like the GPRS can have a huge impact on the way mobile applications are built and in the way they communicate. Dictionary. com defines protocols in the computing field as " a set of rules that govern the format of messages". As mentioned above, encrypting data over communication lines can be a good solution to reducing or in time eliminating the potential security threats of Mobile Banking.

Other solutions involve taking precautions while carrying out mobile banking transactions. Information like bank account details, login and authorization details like passwords and pin codes should be communicated discretely. With mobile applications, the users should never save their authentication details on the mobile phone by deselecting the options for ' automatic logins', and consumers should frequently keep in touch with bank officials in regards to their accounts and services.

SMS technologies can be used by the banking societies to inform their clients of every transaction that takes place with their accounts. This kind of implementation policies can by far reduce the chances of banking fraud since the consumers will be well informed of all the activities that take place regarding their bank accounts. This can benefit both the bank and the consumer. If a bank is known to provide such good services, they will have a larger clientele since average consumers will develop a sense of trust and loyalty with the bank.

Web-wise, WAP technology can be further improved to incorporate security measures like tracking the mobile devices, detecting unusual activities on the sites, and matching the SIM card and mobile phone numbers with the ones their clients provide, to ensure that access to particular accounts can be restricted from unknown numbers. Conclusion

Mobile banking is a breakthrough from Internet banking and it’s actually a great service with many benefits both to banks and consumers. It is a step forward when you look at it from the perspective of technology evolution. It’s very economical in every way to carry out your usual banking transactions merely from a cell phone, however since bank account details and the data the banks store about their clients is sensitive and mostly confidential, it becomes very important to consider the safety of carrying out such operations via wireless networks that can easily be tapped into, by unauthorized parties.

This is the era of new technological innovations, hence such applications are expected; however one must consider how secure they are and how they impact our day-to-day lives. The speed at which technological developments are being implemented every day, there is lots of potential for the banking sector to ensure that the services they provide are fraud-proof.

References

http://www. isaac. cs. berkeley. edu/isaac/gsm. html