ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M13-052013
VOLUME 3 ISSUE 3 May 2013

STRENGTH OF DOUBLE FOLD VERIFICATION

Karun Madan, Surya World Institute of Engg. & Technology, Bapror

Abstract

Today data and information security concerns are getting higher in all areas such as banks, governmental bodies, healthcare field, military operations, educational institutions etc. Government related organizations are forcing standards, passing laws and forcing all organizations and agencies to meet the terms with these standards with non-compliance being met with across-the-board consequences. Today, single fold verification, e.g. passwords, is no longer believed secure in the internet and banking arena. Easy-to-guess passwords, such as birthdays or names of spouse or something similar like age etc, are easily exposed by automated password-collecting series. Double fold verification can meet the requirement of organizations for providing stronger verification options to its end-users. In most cases, a hardware entity is given to each end-user for each account. Consequently, using the cell phone as an entity will make it easier for the consumers to deal with multiple double fold verification systems. In addition, it will trim down the cost of manufacturing, dispensing and maintaining millions of entities.

Introduction

Cell phones have customarily been regarded as a tool for making phone calls. But today, given the advances in hardware and software, cell phones use have been expanded to send messages, check emails, store contacts, etc. Cell phone connectivity options have also increased.

After standard GSM connections, cell phones now have infra-red, Bluetooth, 3G, and WLAN connectivity[1]. End-users have the tendency to use easy-to-guess simple passwords. And moreover, end-user uses the same password in his multiple accounts, write the passwords or store them on their machines or paper etc.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M13-052013
VOLUME 3 ISSUE 3 May 2013

Hackers use many practices to steal passwords such as shoulder surfing, or snooping, or sniffing, some sort of guessing, etc[2]. Several strategies for using passwords have been proposed in recent times. Some of which are very difficult to use and others might not meet the company's security concerns. Double fold verification using gadgets such as entities like ATM cards solve the password problem and have shown to be difficult to hack.

Double fold verification, also have weakness which include the cost of purchasing, supplying and organizing the entities or cards. Most people, if not all of us, carry cell phones for communication purpose. Several cell phone banking services available, improve the potential of cell phone gadgets. From being able to obtain information on account balances in the outline of SMS messages to make use of WAP and Java together with GPRS to permit fund transfers between a variety of accounts, stock trading etc[3].

Issues of Single fold Verification

In verification process, three things need to know are what you should know i.e. passwords, what you must have i.e. some entity or some cards like ATM, and what you actually are (e.g. biometrics like voice, face or gestures. Recent work has been done in trying alternative factors such as a fourth factor, e.g. somebody you should know, which is based on the notion of guarantee [4].

Double fold verification is a mechanism which implements two of the above mentioned aspect and is therefore believed stronger and more secure than the conventionally implemented single fold verification system. Withdrawing money from an ATM machine, employ double fold verification. For this the end-user must possess the unique personal identification number (PIN), i.e. what you know and second, the ATM card, i.e. what you have[5]. Passwords are one of the easiest aims of hackers. Therefore, nowadays most organizations are looking for even more , secure methods to take care of their end-users and employees.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M13-052013
VOLUME 3 ISSUE 3 May 2013

Biometrics are known to be much secure than passwords alone and are used in special organizations, but they are not bring into play much in any kind of secure online transactions or ATM machines due to the high-priced hardware that is needed to identify the end-user/end-user and the maintenance costs, etc[6]. As an alternative, banks and companies are using entities like cards as a mean of double fold verification. A security entity is a physical gadget that an authorized end-user of that particular services, is given to facilitate in verification.

Entities come in two formats: hardware and software. Hardware entities are small gadgets which are small and can be conveniently carried. Some of these entities, store cryptographic keys or some kind of biometric data, while others present a PIN that changes with time. At any particular time, when a end-user requires to log-in to the service, he bring into play the PIN displayed on the entity in addition to his normal account password. Software entities are programs that run on PC and provide a PIN that changes with time.

Using entities involves a number of steps including registration of end-users, entity making and distribution, end-user and entity verification, and end-user and entity revocation among others. While entities offer a much safer environment for end-users, it can be very pricey for organizations[7]. For example, a bank with a million end-users will have to buy, install, and maintain same no. of million entities. Moreover, the bank has to offer continuous support for training end users on how to use the entities.

The banks have to also be geared up to provide replacements if an entity stop working or gets stolen. Replacing an entity is a lot more expensive than substitute an ATM card or resetting a password. From the end-user's prospective, having an account with more than one bank means the requirement to carry and maintain several entities which constitute a big hassle and can lead to entities being lost, stolen, or broken or some other eventuality. In many cases, the end-users are charged for each lost or damaged entity. We suggest a cell phone -based software entity that will save

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M13-052013
VOLUME 3 ISSUE 3 May 2013

the organizations the cost of buys and maintaining the hardware entities[8]. Moreover, will allow end-users to install multiple software entities on their cell phones. Hence, they will only need to worry about their cell phones instead of worrying about several hardware entities.

Cell Phone's Software Entity Realization

End-users seem to be willing to use simple feature such as their cell phone number and a PIN for services such as authorizing cell phone micropayments [9]. Note that these features must exist on both the cell phone and server in order for both sides to generate the exactly same password. In order to secure the system, the generated OTP must be very very hard to guess, retrieve, or trace by the hackers. So, its very important to build up a secure OTP generating algorithm. Several features can be used by the OTP algorithm to produce a difficult-to-guess password. Following features were picked for this:

- **IMEI number:** This is easy to get from the cell phone and will be stored in the server's database for each end-user. The term stands for International Mobile Equipment Identity which is unique to each cell phone allowing each end-user to be identified by his gadget.

- **IMSI number:** It is laid up in the Subscriber Identity Module (SIM) card in the cell phone. This number will also be laid in the server's database for each end-user. The term stands for International mobile Subscriber Identity which is a unique number associated with all GSM or CDMA based systems.

- **End-username:** End-username is used jointly with the PIN to protect the end-user in case the cell phone is stolen. Although no longer mandatory because the IMEI will uniquely identify the end-user in any case.

- **PIN:** This is required to confirm that no one other than the end-user is using the phone to generate the end-user's OTP. In order for the PIN to be tough to guess or brute-forced by the some

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M13-052013
VOLUME 3 ISSUE 3 May 2013

hacker, a minimum of 8-characters long PIN is demanded with a mixture of capital- and small-case characters, digits, and symbols. Note that the end-username and the PIN are never stored in the cell phone's memory. They are just bring into play to generate the OTP and discarded straight away after that[10]. The PIN together with the end-username is data that only the end-user knows so even if the cell phone is stolen the OTP cannot be produced correctly without knowing the end-user's PIN.

- **Hour & Minute:** Hour & Minute permits the OTP generated each hour to be unique. This would make the OTP produced each minute to be unique; hence the OTP would be legitimate for one minute only and might be problematic to the end-user. Note that the software can be customized to allow the administrators to opt for their preferred OTP validity interval. An substitute solution is to only use the first digit of the minute which will construct the password valid for more minutes and will be more handy for the end-users, since some end-users need more than a minute to read and input the OTP.

- **Day & Year/Month/Date:** composes the OTP set unique to each day/month/year. Using the last two digits of the mentioned year and the date and month, create the OTP unique for that specific date. The time is retrieved by the end-user and server from the telecommunication corporation.

The practice results in a password that is unique for a ten minute interval for a specific end-user is as follows. All the above features are concatenated and the end result is hashed using SHA-256 which returns a 256 bit message after this. The message is then XOR-ed with the PIN converted to 256 characters. The result is then Base64 encoded which produces a 28 character message. The message is then reduced in size to an administrator-specified length by separating it into two halves and XOR-ing the two halves again and again.

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M13-052013
VOLUME 3 ISSUE 3 May 2013

Maintaining the password at 28 characters is more safe and secure but more difficult to use by the end-user, since the end-user should enter all 28 characters to some online webpage or ATM machine. The smaller in size the OTP message the easier it is for the end-user, but also the easier it is to be hacked by someone.

A. First Party Design Issues

The code can run on any J2ME-enabled cell phone. The OTP code has the option of producing the OTP locally using the cell phone IMEI and IMSI numbers, or demanding the OTP from the server via an SMS message. The default choice is the first method which is cheaper since no SMS messages are swapped over between the end-user and the server. However, the end-user has the choice to select the SMS-based method. A J2ME code is developed and installed on the cell phone to produce the OTP. The program has an simple - to-use GUI that is produced using the NetBean's drag and drop interface.

B. Second Party Design Issues

The password area will store the hash of the 10 minute password. It will not save the password itself. Should the database be conciliation the hashes cannot be inverted in order to get the passwords used to produce those hashes. Hence, the OTP algorithm will not be marked out. A database is required on the server side to store the end-user's identification knowledge such as the first name, last name, end-username, pin, simple password, cell phone IMEI number, IMSI number of mobile and unique symmetric key.

C. Server Design Issues

The server consists of a database and is linked to a GSM modem for SMS messages swap. A server is implemented to produce the OTP on the organization's side. The software is configured to link to the server's GSM modem in case the SMS based choice is exercised. A unique symmetric key is also produced and

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers

International Refereed and Indexed Journal for Research Scholars and Practitioners

http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M13-052013
VOLUME 3 ISSUE 3 May 2013

installed on both the cell phone and also the server.

Conclusion

As data security concern comes to one's mind, the word password flashes to mind. Nowadays almost all systems today rely on inactive passwords to verify the end-user's distinctiveness. But the problem with such approach of passwords, come with major management as well as security concerns. End-users have the tendency to use easy-to-guess simple passwords. And moreover, end-user uses the same password in his multiple accounts, write the passwords or store them on their machines or paper etc. Hackers use many practices to steal passwords such as shoulder surfing, or snooping, or sniffing, some sort of guessing, etc. Double fold verification using gadgets such as entities like ATM cards solve the password problem and have shown to be difficult to hack. Double fold verification, also have weakness which include the cost of purchasing, supplying and organizing the entities or cards. From the end end-user's point of view, using more than one double fold verification system requires carrying multiple entities which are prone to get lost or stolen. Since many end-users carry a cell phone today at all times. So, with this provision, double fold verification makes its way by replacing cell phones with other entities like cards etc.

References

[1] B. Schneier, "Two-Factor Authentication: Too Little, Too Late," in Inside Risks 178, Communications of the ACM, 48(4), April 2005.

[2] D. Ilett, "US Bank Gives Two-Factor Authentication to Millions of Customers," 2005. Available at http://www.silicon.com/financialservices/0,3800010322,39153981,00.htm

[3] D. de Borde, "Two-Factor Authentication," Siemens Enterprise Communications UK- Security Solutions, 2008. Available at http://www.insight.co.uk/files/whitepapers/Twofactor%20authentication%20(White%20paper).pdf

ISSN (Online) : 2249 - 054X
International Journal of Computing and Corporate Research
Multi Disciplinary Journal for Publication of Review and Research Papers
International Refereed and Indexed Journal for Research Scholars and Practitioners
http://www.ijccr.com
International Manuscript ID : ISSN2249054X-V3I3M13-052013
VOLUME 3 ISSUE 3 May 2013

[4] A. Herzberg, "Payments and Banking with Mobile Personal Devices," Communications of the ACM, 46(5), 53-58, May 2003.

[5] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo and M. Yung, "Fourth-Factor Authentication: Somebody You Know," ACM CCS, 168-78. 2006.

[6] NBD Online Token. Available at http://www.nbd.com/NBD/

NBD_CDA/CDA_Web_pages/Internet_Banking/nbdonline_topbanner

[7] N. Mallat, M. Rossi, and V. Tuunainen, "Mobile Banking Services," Communications of the ACM, 47(8), 42-46, May 2004.

[8] "RSA Security Selected by National Bank of Abu Dhabi to Protect Online Banking Customers," 2005. Available at http://www.rsa.com/press_release.aspx?id=6092

[9] R. Groom, "Two Factor Authentication Using BESTOKEN Pro USB Token." Available at http://bizsecurity.about.com/od/mobilesecurity/a/twofactor.htm

[10] Sha.J. Available at http://www.softabar.com/home/content/view/46/68/