KEY LOGGING RESILIENT FOR VISUAL AUTHENTICATION PROTOCOL

PAMPANA SIRI VENNELA [#1], L. SOWJANYA [#2]

[#1] MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

Now a day's security plays a very important role in each and every aspect of human life. As security plays a very important role in all aspects of life, a lot of illegal users try to access the information of others illegally. To avoid this there was various new techniques proposed in order to store the data safely on remote machines.Eventhough there was no mechanism which clearly provides complete security over the local and remote system storage. So the design of a secure authentication protocols is quite challenging problem in the recent days. Till now almost each and every user try to provide security only user username and password, it doesn't achieve high security because of guessing or dictionary attacks. In this application we have implemented a novel security system by involving the visual authentication protocols for storing the data safely inside the system. For this we have taken image as primary security for storing and accessing the data.

1. INTRODUCTION

Threats against electronic and financial services can be classifiedinto two major classes: credential stealing and channel breaking attacks [20]. Credentials such as users' identifiers, passwords, and keys can be stolen by an attacker when they are poorly managed. For example, a poorly managed personal computer (PC) infected with a malicious software (malware) is an easy target for credential attackers . On the other hand, channel breaking attacks—which allow for eavesdropping on communication between users and a financial institution—are another form of exploitation. While classical channel breaking attacks can be prevented by the proper usage of a security channel such as IPSec and SSL (secure sockets layer) , recent channel breaking attacks are more challenging. Indeed, "keylogging" attacks— or those that utilize session hijacking, phishing and pharming, and visual fraudulence— cannot be addressed by simply enabling encryption. Chief among this class of attacks are keyloggers . A keylogger is a software

designed to capture all of a user's keyboard strokes, and then make use of them to impersonate a user in financial transactions.

KEYLOGGERS

Keyloggers, or keystroke loggers, are ingenious software programs or hardware attachments, used mainly for identity theft. Very simply, they record all the keystrokes a user inputs. The data is then either sent across to a person on the other end, or stored for later retrieval. However, like everything else, keyloggers have evolved greatly and are now capable of recording almost anything on the computer – right from voice conversations to clipboard contents [2].

TYPES OF KEY LOGGERS

1) Hardware Key loggers

The other large category is hardware-based keyloggers, which serve the same purpose, but are fundamentally different in the way of achieving their goal. They are fully self-contained hardware units that are attached to the computer, most usually as a plug between the keyboard and the computer, and they require no software to be set up. Different to software keyloggers, all the data is stored on the piece of hardware, and it never appears on the computer that is being monitored. Consequently, the only way to retrieve the stored data is by retrieving the hardware unit itself. As the data is not stored on the computer, it can't be accessed while the keylogger is working, nor is it vulnerable to anti-spyware software or hard drive crashes, which would usually erase software keylogger data[2]. Hardware keylogger is inserted between the keyboard and the USB (or PS/2) port. It also contains its own CPU to avoid drawing on the resources of your computer. Some of the USB keylogger devices are equipped with WiFi so you can access the data by logging into your email account.

2) Software Key loggers

Keylogger software is a program that you download and install on your PC. It is often downloaded from reputable websites for the purpose of monitoring the computing activity of your child, employee, or as a means of retrieving your data in the event your PC crashes. When you download keylogger software it runs in stealth mode which means it is invisible to the PC user.

Although the software is installed on the hard drive it is not visible if you look for it in any files or folders. Instead it takes a password in order to make it visible. Keylogger software is capable of sending logs of recorded data to your email account or a File Transfer Protocol address on a local server where you can access it.

With some programs that are used for parental control you can also block questionable websites and applications that
you do not want your child to access.

Regardless of whether your use a hardware keylogger or a keylogger software it is important to be aware that it can be used for positive purposes or negative purposes. The proper way to use keyloggers is for the good and the positive [3].

2 . LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into for developing the proposed system.

DaeHun Nyang, proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication protocols. They have shown two realizations of protocols that not only improve the user experience but also resist challenging attacks, such as the keylogger and malware attacks. Proposed protocols utilize simple technologies available in most out-of-the-box smart phone devices. Author developed Android application of a prototype of our protocol and demonstrate its feasibility and potential in real-world [5].

M. Mannan, has implemented a simple approach of Mobile Password Authentication. While PC's tend to dominate transaction processes they are vulnerable to various forms of attacks so they have used an intermediate device in the form of mobile and hence security is not entirely dependent on PC's [6].

Haichang Gao, have put forth the idea of including graphical password strategy for authentication. Their paper presents the idea that long alphanumeric passwords are hard for people to remember while shorter is easy to crack so a conclusion is to include graphical password [7].

R Divya, proposed system consisting of two protocols for authentication which resisted keylogging. The two authentication protocols are Time based One-Time- Password protocol and Password-based authentication protocol. Their proposed system shows how visualization can enhance usability and security[8].

3. EXISTING SYSTEM

The design of secure authentication protocols is quite challenging, considering that various kinds of root kits reside in PCs (Personal Computers) to observe user's behavior and to make PCs untrusted devices. Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization. Therefore, relying on users to enhance security necessarily degrades the usability. On the other hand, relaxing assumptions and rigorous security design to improve the user experience can lead to security breaches that can harm the users' trust. Also in the existing system there was no system with more than one type of visual authentication protocols for giving security for the sensitive data.

LIMITATION OF EXISTING SYSTEM

The following are the limitation of the existing system :

1. It is non Security for Stored data.
2. In the existing there was no method of integration more than one visual authentication protocols for giving security.
3. In the existing system there was no mechanism which uses pattern along with image as authentication.
4. In the existing system there was no system that integrates password authentication along with image click based authentication.

4. PROPOSED SYSTEM

In this Project, we demonstrate how careful visualization design can enhance not only the security but also the usability of authentication. To that end, we propose three visual authentication protocols: one is a user name and password authentication, second is image as authentication by matching image pixels and the other is a pattern as authentication protocol. Through rigorous analysis, we verify that our protocols are immune to many of the challenging authentication attacks applicable in the literature. Furthermore, we also extended the application with another level of security like image click points as authentication ,so that by combining all these factors gives a utmost security for the sensitive data.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system :

1. It is having full Security for the Stored data.
2. In the proposed system there was a method of integration more than one visual authentication protocols for giving security.

3. In this proposed system there was a mechanism which uses pattern along with image as authentication.

In this proposed system as an extension we have integrated password authentication along with image click based authentication.

5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed protocol. The proposed application is mainly divided into 5 modules. They are as follows:

1. Load Disease Data Set
2. User Module
3. Machine Learning Technique
4. Identify Disease using Rule Based Expert System
5. Identify Disease using Machine Learning Algorithm

Now let us discuss about each and every module in detail as follows:

5.1 Load Plant Dataset Module

This is a predefined task which is done by the administrator in order to maintain a proper data set to classify the plant diseases. Whenever a new plant disease is invented, then that disease details should be maintained into the database by the administrator. This is nothing but collecting training data set information for the naïve bayes classification algorithm.

5.2 User Module

In this module the user is one who try to verify the diseases on a plant. he try to identify all the infected areas of that plant physically and then try to substitute those symptoms on that plant library. Here those symptoms which he found will be choose as yes and remaining those symptoms which he didn't observe on that plant will be selected as No. So once after choosing all the values the corresponding inputs is send to the ML approach. Here the user try to give test inputs for the Naïve Bayes classification

algorithm. These test values should be matched with training data set and then probability of disease is identified by the ML approach.

5..3 Machine Learning Technique Module

In this module, the predefined disease data sets and user inputs are to be learned by the machine (computer). Machine learning is the study of how to make computers learn; the goal is to make computers improve their performance through experience. This ML is mainly used in clustering the diseases based on the type of symptoms. As we all know that all plants may not suffer with same type of disease and same level of complaints. So based on the individual problem ,the ML system need to guide the user to take cure on those conditions.

5.4 Rule Based Expert Module

Here the diseases can be identified based on rule based expert system which means user need to input the symptoms based on the one of the 5 levels and after the user choose the level and enters all the symptoms then only the user will get the appropriate disease name based on expert knowledge. Here if the user choose all symptoms as null, then the resultant output will be displayed as no disease for that plant. If the same user try to choose appropriate inputs then based on that the disease will be predicted and cure will be provided for that user.

5.5 Machine Learning Based Module

Here this module clearly tells that there is no need to choose individual category and then input the symptoms. If the user find some common symptoms which can be generally visualized and identified. Those symptoms he try to choose from this common list of attributes and based on those fields ,the ML approach will decide which type of disease the plant suffer from and how much percentage of infection occurred to the plant. We can calculate the percentage of infection on that plant.

6. EXPERIMENTAL RESULTS

Home Page

User Should Register First in order to get access the system

User fills all his registration details

Now user should browse an image ,this image acts as a security primitive for this entire application

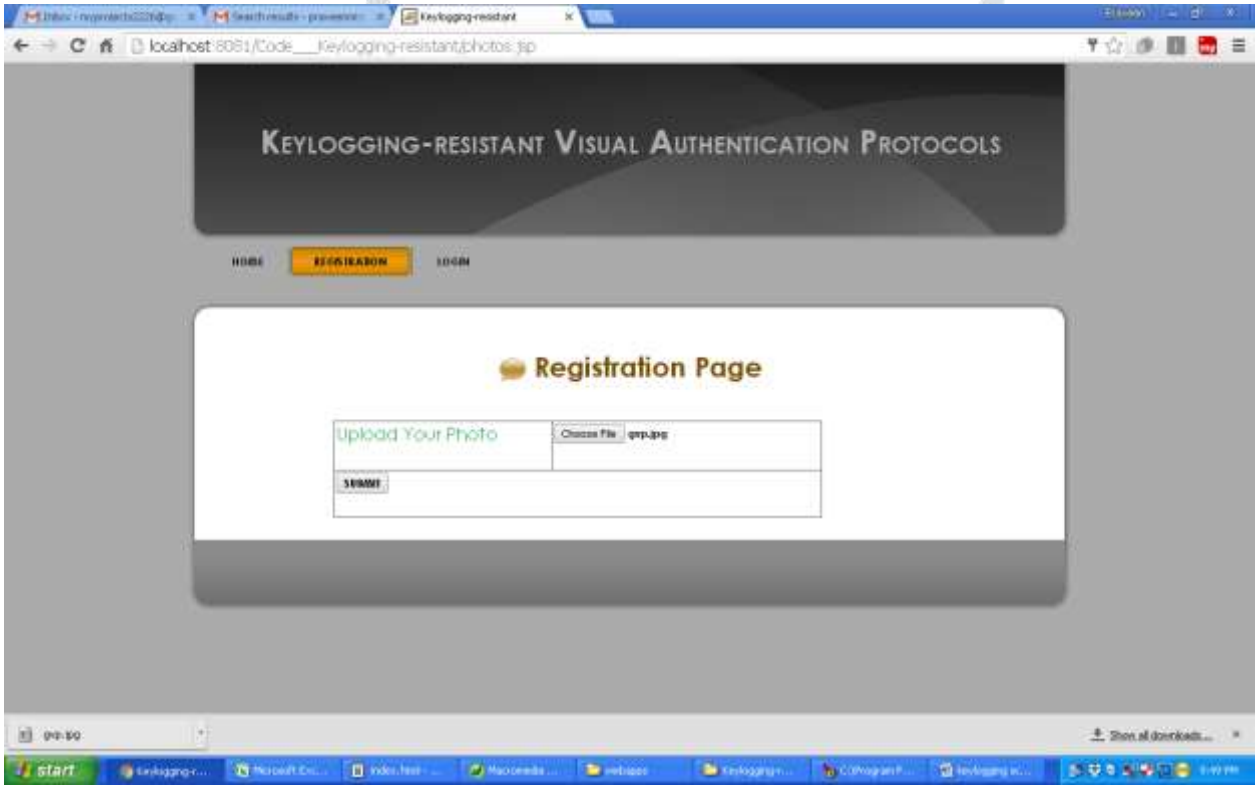


Image is uploaded into the site

Now users should click on any one image which is appeared automatically by the system

Registration is success

User login main page

Once user enters his valid id and password ,then he will enter into the second phase for authentication

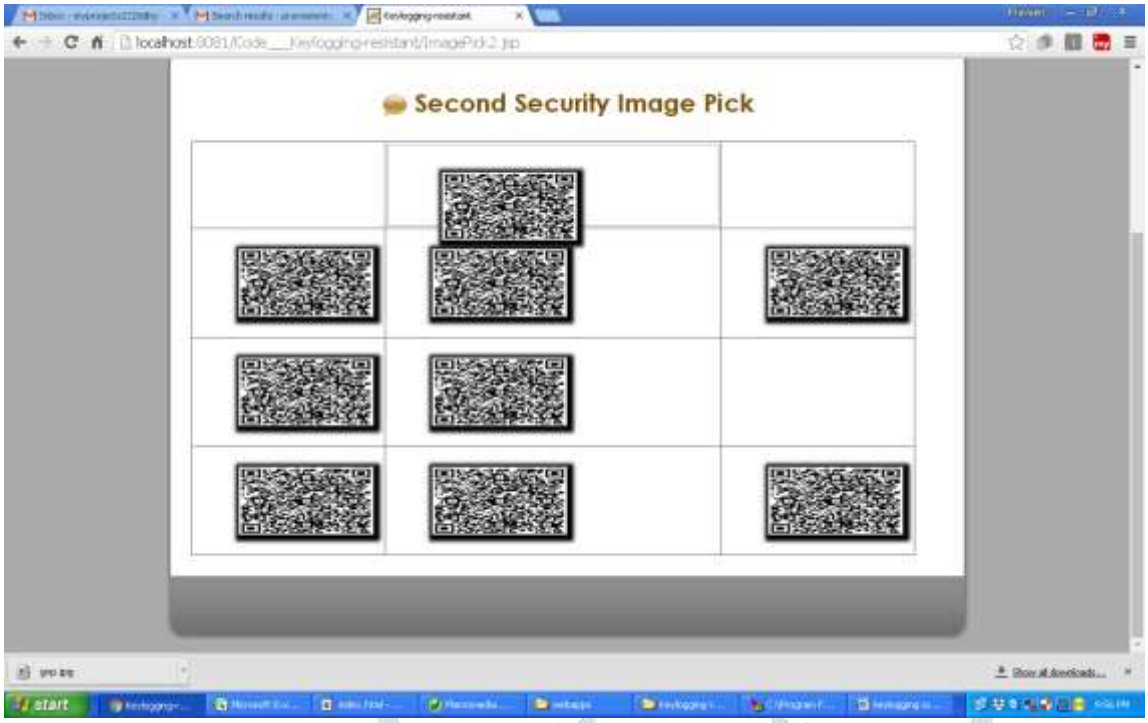
Here the user GVP has uploaded an sample image into the site during registration. So he need to choose the same image in order to enter into the next level of authentication

Now after satisfying second level of security he need to click on same image what he has choosen at the time of registration

Final level of security that is pattern which acts as fourth level of security

First position drag

Second Drag

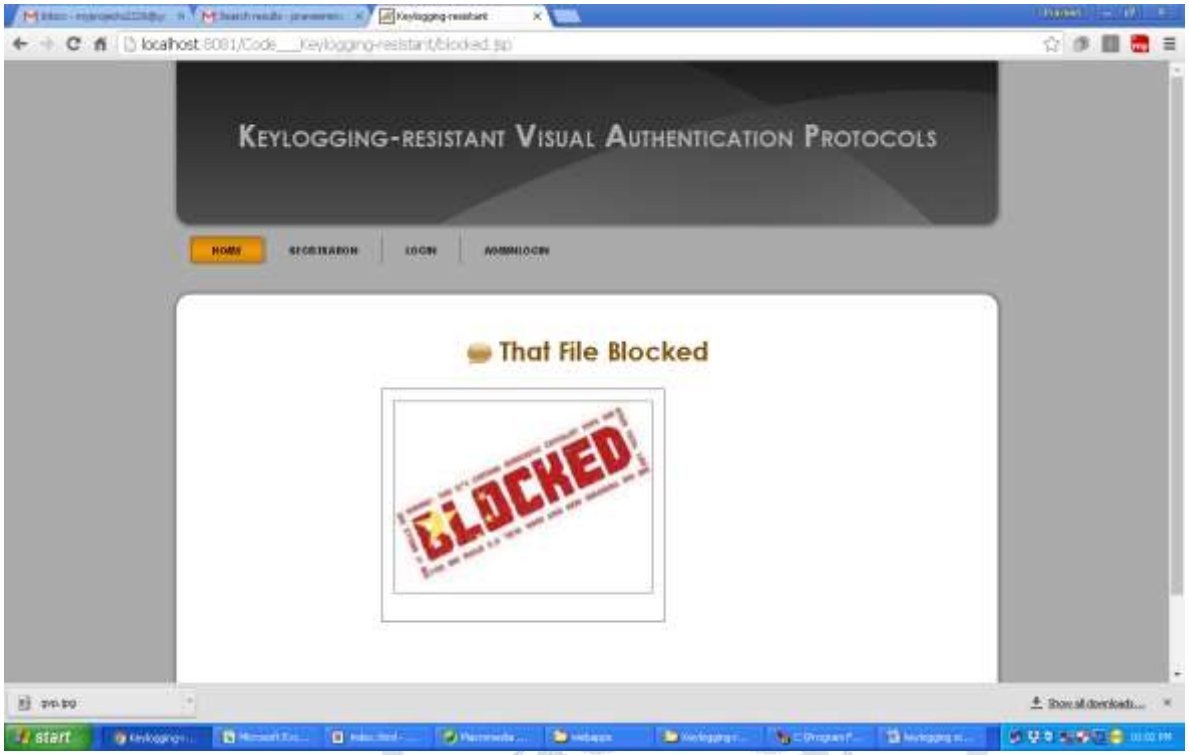


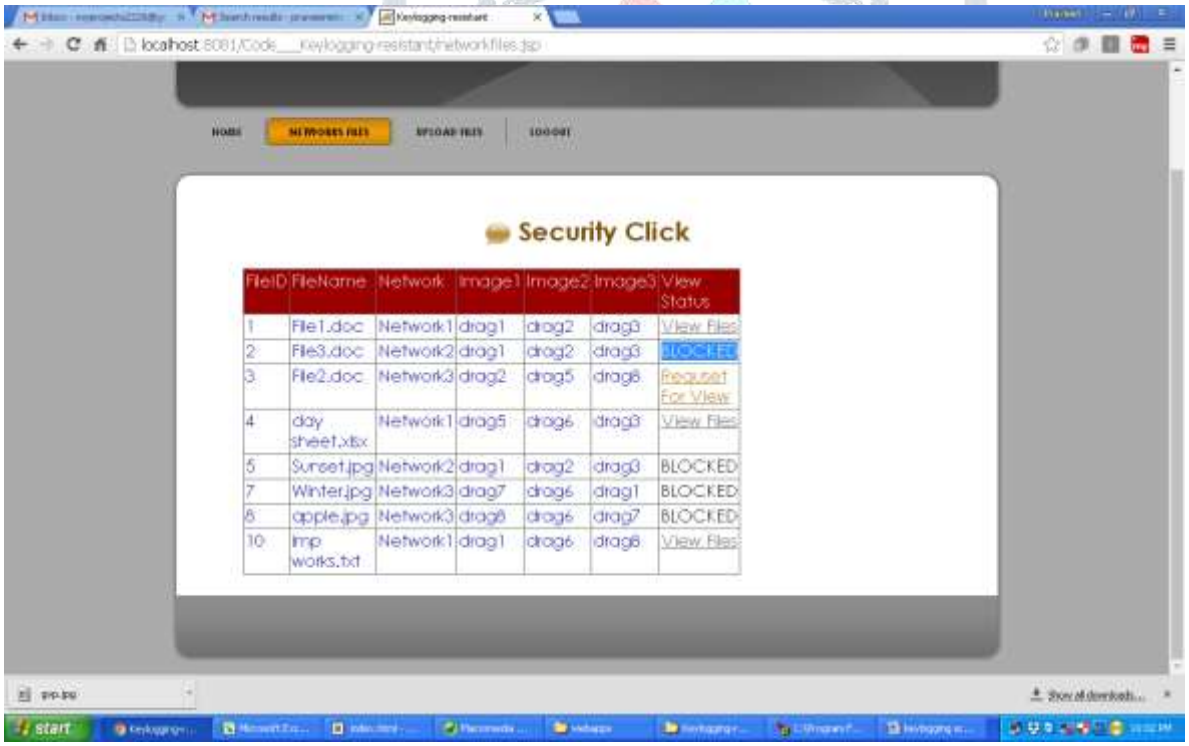
Third Drag

After three drags the file is successfully uploaded

User can view the files what he uploaded directly but if the same user want to view others files of other network..He need to request the admin

Account blocked if he substitutes wrong pattern





7. CONCLUSION

We proposed and analyzed the use of user driven visualization to improve security and user-friendliness of authentication protocols. Moreover, we have shown two realizations of protocols that not only improve the user experience but also resist challenging attacks, such as the key logger and malware

attacks. Our protocols utilize simple technologies available in most out-of-the-box smartphone devices. We developed Android application of a prototype of our protocol and demonstrate its feasibility and potential in real-world deployment and operational settings for user authentication. Our work indeed opens the door for several other directions that we would like to investigate as a future work. First of all, our plan is to implement our protocol on the smart glasses such as the google glass, and conduct the user study. Second, we plan to investigate the design of other protocols with more stringent performance requirements using the same tools provided in this work. In addition, we will study methods for improving the security and user experience by means of visualization in other contexts, but not limited to authentication such as visual decryption and visual signature verification. Finally, reporting on user studies that will benefit from a wide deployment and acceptance of our protocols would be a parallel future work to consider as well.

8. REFERENCES

[1] Google authenticator. http://code.google.com/p/ google-authenticator/.

[2] Rsa securid. http://www.emc.com/security/rsa-securid.htm.

[3] Cronto. http://www.cronto.com/.

[4] BS ISO/IEC 18004:2006. information technology. automatic identification and data capture techniques. ISO/IEC, 2006.

[5] ZXing. http://code.google.com/p/zxing/, 2011.

[6] D. Boneh and X. Boyen. Short signatures without random oracles. In Proc. of EUROCRYPT, pages 56–73, 2004.

[7] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 553–567. IEEE, 2012.

[8] J. Brown. Zbar bar code reader, zbar android sdk 0.2. http://zbar. sourceforge.net/, April 2012.

[9] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer,A. Perrig, B.-Y. Yang, and T.-C. Wu. Gangs: gather, authenticate ’n group securely. In J. J. Garcia-Luna-Aceves, R. Sivakumar, and P. Steenkiste, editors, MOBICOM, pages 92–103. ACM, 2008.

[10] S. Chiasson, P. van Oorschot, and R. Biddle. Graphical password authentication using cued click points. In Proc. of ESORICS, 2008.

[11] D. Crockford. The application/json media type for javascript object notation (json). http://www.ietf.org/rfc/rfc4627.txt?number=4627, July 2006.

[12] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In Proc. of USENIX Security, 2004.

[13] N. Doraswamy and D. Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall, 2003.

[14] M. Farb, M. Burman, G. Chandok, J. McCune, and A. Perrig. Safeslinger: An easy-to-use and secure approach for human trust establishment. Technical report, CMU, 2011.

[15] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu. Yagp: Yet anothergraphical password strategy. In Proc. of ACM ACSAC, pages 121–129, 2008.

[16] S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal, 1988.

[17] Google. Android. http://www.android.com/, 2011.

[18] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig. Use your illusion: secure authentication usable anywhere. In Proc. of ACM SOUPS, 2008.