Latest Approach to Improve the Protection of Embedded Systems by Using PGP Technique

P. Rama Bayapa Reddy, K. Soundararajan, and M. H. M. Krishna Prasad

***Abstract*—In today's world of ubiquitous computing, cyber attacks are becoming more virulent, costlier, and larger in scope than ever before. Unlike previous incarnations of hacking, current attacks on computer systems are professionally coordinated, multifaceted, and motivated by the promise of profits on a massive scale. With millions of new electronic devices connecting to the internet every day, hackers are increasingly focused on a new type of target: mobile and embedded systems. Such systems include point-of-sale terminals, wireless routers, smart phones, networked office machines such as printers, and even the utility infrastructure. Pass points scheme is one of the techniques used in Authentication using Graphical Images. In this method, users click on images rather than typing a long and complex alphanumeric password with the computer keyboard. Psychological studies have shown that people can remember pictures better than text. During the time of registration a user may choose several areas (click points) on an image. In order to log in the user has to click close to the chosen click points, e.g. within 0.25cm to 0.50cm from the click point, because users cannot click exactly on the same pixel on which they have clicked at the time of registration. This margin of error around the click point is called Tolerance. Existing Pass points scheme uses a fixed tolerance (say 20X20 pixels) over a number of clicks by the user. But by varying the tolerance (i.e., decrementing the tolerance level) as users click on more points, the information left to an attacker is reduced. We have also introduced multiple graphical passwords approach to counter shoulder surfing attack. Cutting-edge hackers are acutely aware that many of the security procedures and applications in use today have been designed for PC workstations, and are thus unable to thwart attacks on mobile and embedded systems. Smart phones, for example, remain notoriously insecure, yet they are gaining popularity as platforms for exchanging confidential data and conducting financial transactions. Billions of dollars are at risk as people do more and more of their everyday banking and shopping on mobile and wireless devices. Even heart pacemakers have joined the networked world and are now vulnerable to hacking.**

***Index Terms*—Authentication, graphical passwords, multiple passwords, pass points scheme, tolerance.**

I. Introduction

Perhaps most ominous of the new hacking trends is the upsurge in cyber attacks against our utility infrastructure. If hackers continue to attack the so-called "smart grid," which connects sensors and control systems with sophisticated computers and networks, they could bring our nation's commerce to a standstill, endanger lives, and put our national security at risk. Now a days, all business, government, and academic organizations are investing a lot of money for the security of information. In this dangerous new interconnected world, we need to take a serious look at what types of hacking strategies are being employed today, and implement security solutions that are designed specifically for mobile and embedded devices. This paper attempts to highlight some of the latest attacks against embedded systems, including mobile phones, medical devices, and the nation's electric infrastructure. A key area in securing the valuable information authentication.

What is Authentication? Authentication refers to the process of verifying the Identity of a communication partner. It determines whether a user is allowed to access a particular system or resource. Today it is a critical area of security research. Authentication techniques can be classified into three categories. They are

1) Token based authentication
2) Biometric based authentication
3) Knowledge based authentication

The classification is shown in Fig. 1. The best example for token based authentication is a bank cards like credit or debit. Some authentication systems also use knowledge based authentication technique to enhance the security of information. For example, ATM debit cards generally require a PIN number which is to be remembered by the user.

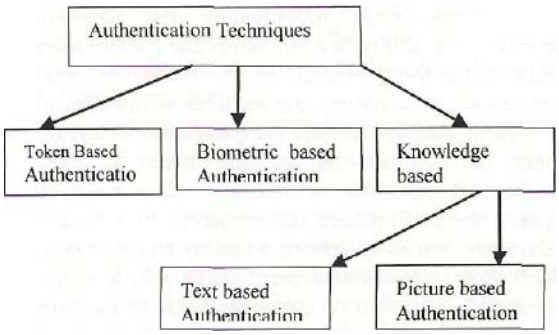

Fig. 1. Classification of authentication techniques

Fingerprints, Iris scan, voice recognition, hand geometry are comes under Biometric Authentication. But the drawback of this approach is that the systems and equipment used for verifying the authenticity are not only expensive but the process is slow. However, this technique has a high level of security. Finally, Knowledge based techniques are

Manuscript received September 16, 2012; revised October 27, 2012.

P. Rama Bayapa Reddy is with the Dept. of CSE, Dhruva Institute of Engineering and Technology, Hyderabad, India (e-mail: . putluru.ramreddy@gmail.com)

K. Soundararajan is with the Department of ECE, JNTUACE, of Jawaharlal Nehru Technological University College of Engineering, Anantapur, A.P, India,

M. H. M. Krishna Prasad is with the Dept. of Information Technology University College of Engineering JNTUK–Vizianagaram, A.P, India.

DOI: 10.7763/IJFCC.2013.V2.134

the most commonly used techniques. Knowledge based techniques are classified into two categories. They are text based passwords and picture based passwords [4]. The picture based authentication techniques are further divided into two categories. They are recognition-based graphical techniques and recall based graphical techniques. In recognition based technique, a user is given a pool of images and the user has to recognize and identify the images, which he or she selected during the time of registration. In recall based techniques, the user has to reproduce something he or she created at the time of registration.

II. Graphical Passwords

Graphical passwords are an alternative to existing alphanumeric passwords. In graphical passwords users click on images. Prior to the graphical passwords, the most common authentication method is a 'Password', which is an alphanumeric word known to the computer and the user. The results of a recent survey shows that 93% of large businesses in United Kingdom still use passwords to authenticate users [4] .But users have many problems with the alphanumeric passwords like users have difficulty remembering complex, pseudo-random passwords overtime.

HACKING DETAILS: Years ago, hacking was an amateur, underground activity, commonly associated with thrill-seeking pranksters whose main intent was showing off their computing prowess or expressing their anti-authoritarian sentiments. To be a hacker was to have "street cred"—at least among the technologically savvy. Although hackers' activity was often illegal it was rarely malicious, and they usually didn't fit the profile of career criminals. Generally, a 'good' password has some characteristics like including numbers, alphabets (both capital and small) and special symbols, and not only that it must be long enough to stand against different attacks. Such pseudo-random passwords lack meaningful content and can be learned only by rote memorization, a weak way of remembering [16]. Studies have shown that users tend to pick short passwords or passwords that are easy to remember [1],According to Computerworld news article, a team of security engineers ran j password cracker in a network and within 30 seconds, they cracked 80% of the passwords [12].

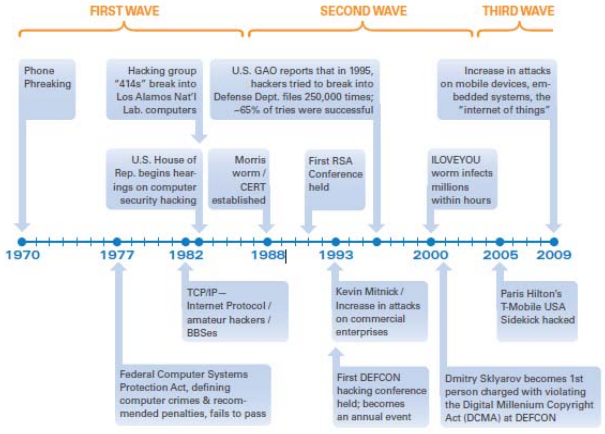

Fig. 2. Hacking timeline

People often forget their passwords. If a password is not - used frequently it will be even more susceptible to forgetting. If the password is hard to guess, it is hard to remember. Psychological theories have identified decay over time and interference with other information in long term memory as underlying reasons for forgetting [9]. Another complicated issue is that users have many passwords for computers, networks and e-mails. Remembering a complex and long password is difficult. But Studies shows that human brain can better recall images than text [1]-[5]. Some of the early hackers of the 1970s focused on the telephone system. Calling themselves [phone] "phreaks," or "phreakers," they helped themselves to free long distance by simulating the sounds of phone signals. In the 1980s, when personal computers became widely available, phone phreaks and other hackers began using modems to connect to Bulletin Board Systems (BBSes), where they exchanged messages about how to break into computers, steal passwords, and wreak other kinds of electronic havoc. By 1986, hackers had threatened enough government and corporate computer systems to prompt the U.S. Government to make hacking a crime. In 1988, foreshadowing the types of attacks that lay ahead, ArpaNET, the U.S. government's precursor to the internet, was brought to a standstill by a hacker's experimental, self-replicating "worm" program that spread to 6000 of the network's computers. Further studies on images shows that images are recognized with very high accuracy (up to 98%) after a two hour delay, which is much higher than accuracy for words and sentences [5]. In addition, it has been found that errors in recognition of images are only 17% after viewing ten thousand pictures [19]. Studies of recall also confirm that pictures are recalled better than words, and this has led to the "picture superiority effect [12]. That is pictures are superior in remembering and recognizing.

III. Background on Graphical Password Systems

Apart from Pass point's technique [12], other techniques are also available [3]-[6]-[2]. One such technique is Pass faces [19], in which user chooses four faces from a pool of faces. When logging in, the user sees a 3X3 grid of nine faces, consisting one face previously chosen by the user and eight decoy faces, the user has to recognize and click anywhere on chose n face. This procedure is repeated with different target and decoy faces, for a total of four rounds. It is observed that pass faces may be more memorable than alphanumeric passwords [5]. Another similar system is proposed [7] which suggest that choosing images from a pool of images is a slow process, but the images are easier to remember. Passlogix [2] has developed a similar system. In their method, users must click on areas in the correct sequence in order to be authenticated. Invisible boundaries are defined for each clicked area in order to detect whether a particular area is clicked by the mouse. A similar technique was developed by sfr [14]. The software giant Microsoft has also developed a comparable graphical password technique where users are required to click on pre-selected areas of an image in a chosen sequence [14]. Hacking's Dangerous Third Wave: Now, with the advent of what some technologists call the "internet of things" (Fig. 3), we are encountering a third wave of hacking—one that encompasses not only wired computers and networks, but

intelligent devices like wireless phones, routers and switches, printers, SCADA (Supervisory Control And Data Acquisition) systems, and even medical devices. This new hacking wave is poised to bypass the amateur "street-cred" phase and move directly to well-honed, massively coordinated, sophisticated attacks. It is now becoming clear that hacking's below Fig. 3 third wave will almost certainly include terrorist cyber strikes against the utility and industrial infrastructure (the "smart grid")—a danger we can no longer dismiss as a spy movie scenario.

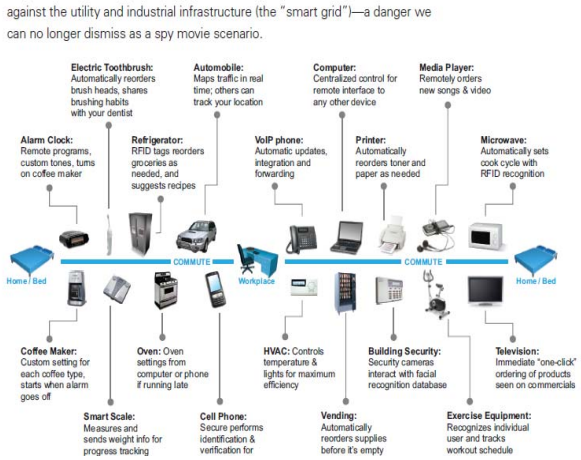

Fig. 3. Hacking's third wave

IV. Pass Points System

The pass points system by Wiedenbeck, et al., [16], [19], is based on the idea of Blonder [3] in which the password is represented by multiple clicks on a single image. But pass points system overcame the limitations of his (Blonder) scheme, i.e., there are no predefined boundaries around areas of the image where the user can click. One of the advantages with pass points scheme is that a user can click on anyplace in the image as a click point. It allows the use of arbitrary images. After clicking on several places (pixels) the sequence is stored. A tolerance region around the chosen click points is calculated. When logging in, the user has to click on points within the tolerance. There is another method in which a single click on multiple images is allowed. It is called as Cued Click Points. These schemes are called as cued recall based schemes since the background image can be regarded as a cue to recall the location of clicks chosen as a password. Cued recall based schemes are different from recognition based schemes in one important aspect. Their password space (e.g., 213) [3]-[6] is larger than the space in recognition based schemes (e.g. 10000 [7]). So recognition based schemes are generally not suitable for Internet applications where brute force attacks are possible. Long-Predicted Threats to Cellular Network & Smartphones Manifesting Themselves Researchers are predicting that 2009 will be a significant year for mobile attacks [H10]. The latest mobile phones are also the most vulnerable to attack. Smart phones, such as the Apple iPhone and the Google Android phone, now come with "real" browsers with JavaScript engines, exposing them to traditional browser attacks, such as Cross-Site Scripting (XSS), Click jacking, phishing, and other malicious techniques. These phones are also vulnerable to "man-in-the-middle" attacks, in which a hacker could come between the phone and a web server and offer malware in the guise of a legitimate update to one of the user's trusted applications. Other vectors for smart phone attacks include email, attachments, web pages, MMS, Face book, Wi-Fi, and Bluetooth [M3].

V. Advantages of Pass Points System

An image which is populated with many objects has hundreds of memorable points, which means that the pass point's scheme provides a large password space when compared with an alphanumeric password. For examples an image with the size of 350X280 mm2 with tolerance region of size 5X5 mm2 and assume that nearly quarter of the image consists of memorable places, we can get 980 memorable tolerance regions. If a user selects five click pointes, then this leads to 9805 memorable passwords, which has a very large password space. Another observation is that, for alphanumeric passwords of length 5 over a 64 character alphabet, the number of possible passwords is 645.Pass Points scheme also provides protection against key logger spy ware. A key logger captures all keystrokes that the user types on the computer keyboard, including passwords, personal information entered into an online registration form (e.g., a mailing address or telephone number), and financial information submitted as part of an online transaction, and the contents of emails or instant messages. Pass Points scheme protects us from key loggers.

VI. Effects of Varying Tolerance

This system is implemented as a web application, where images are stored at server side. If a new user wants to register, he/she will be given a set of eight images (Fig 4).

From these eight images, user has to select one image and then click on one or more areas as a graphical password. Users should remember the order of clicks and they have to produce the same order when they log in. Size of images used in our application is 431×540. We modified original images in such a way that some English alphabets are added on the background of the image where background is plain and clear. Now users can click not only on the areas of objects but also on areas where alphabets are present and they can even select small areas (Fig 3). Studies shows that images that are pleasant and have positive affect may support memorability [4].The original pass points system used a constant tolerance over several click points. But we observed that by varying the tolerance i.e., by decreasing the tolerance level as the user click on more points, it has become more secure. We implemented the system with the first four clicks the tolerance is 20X20, but from then onwards for every two clicks the tolerance is decremented.

In our experiment, we observed that most of the users are interested to have six to eight clicks. So, we gave high tolerance to the first four clicks and from then onwards the tolerance levels are decremented. If a third person observes our clicks and try to reproduce the same after some time he/she may not succeed because for first four clicks the tolerance is same and for next two clicks onwards a clear observation is needed. For example, if user selects only four click points the results are same for the existing system and

our system. But if the user selects more than four clicks then security is enhanced i.e. if the user selects six points then in the existing pass points system the same tolerance for all six points is used. When we compare this with our system attacker gets information which is reduced by near/ 152pixels(76+76). Another example with eight click points is iterance is used in the existing pass points scheme but to shoulder surfing attacks, some extent our method provides the reduced tolerance levels the information left to attacker is reduced by nearly 288 pixels In this fashion if user selects more clicks in his graphical password, information left to an attacker is reduced by more number of pixels. It is shown in Fig.6

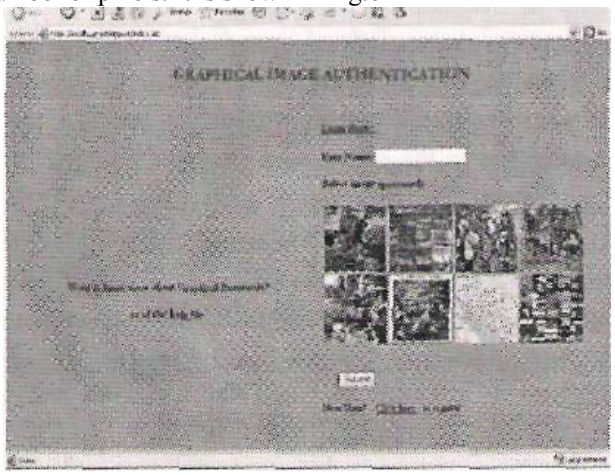

Fig. 4. A screen shot of login page

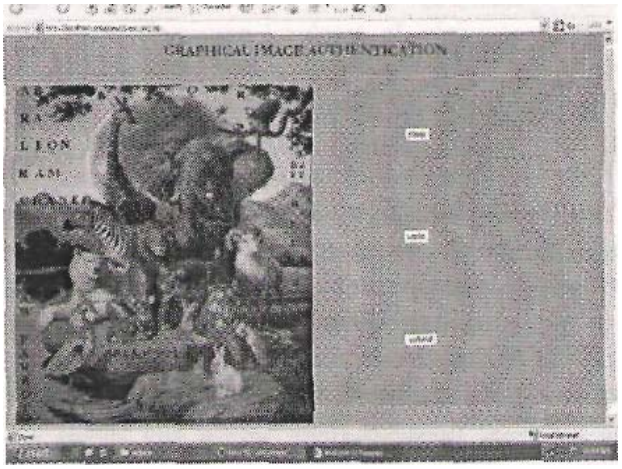

Fig. 5. A screen shot of modified image for clicking

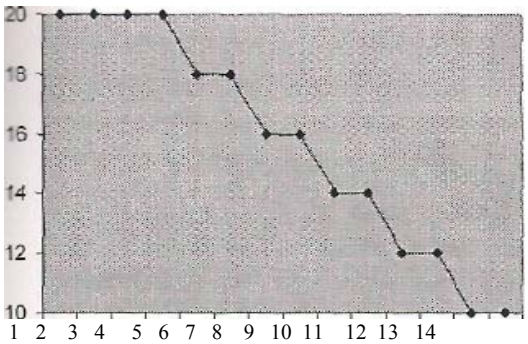

Fig. 6. Varying tolerance through number of clicks

This system could have been implemented in other way i.e. continuously decreasing the tolerance levels over the number of clicks. But we observed that psychologically users are keeping in mind that they should choose only small and specific objects, so, it leads to a slow clicking process. Based on Fitts' Law [9] we expect slower input times in graphical password systems, if the input involves mouse movement and a small tolerance.

VII. Conclusion and Future Work

A major advantage of Pass Points scheme is its large password space over alphanumeric passwords. But the security of Pass Points system is also an important issue. We observed that by varying the tolerance levels, we leave less information to the attacker. Although graphical passwords are vulnerable.

References

[1] A. Adams and M. A. Sasse, "Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures," *Communications of the ACM*, vol. 42, pp. 41-46, 1999.

[2] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings of Midwest Instruction and Computing Symposiutn*, 2004.

[3] B. G. G. Passwords, In *Lucent Techno logics*, Inc., Murray Hill, NJ, U.S Patent, Ed. United States,1996.

[4] M. M. Bradley, M. K. Grenwald, M. C. Petry, and P. J. Lang, "Remembering pictures: Pleasure and arousal in memory," *Journal of Experimental Psychology*, vol. 81, no. 2, 1992, pp. 379-390.

[5] S. Brostoff and M. A. Sasse, "Are Pass faces more usable than passwords: A field trial mvestication, in *people and Computers XIV-Usability or Else*.

[6] S. Chiasson, A. Forget, R. Biddle, and P. C. Van, "Oorschot Influencing User Towards Better Passwords: Persuasive Cued Click-Points," 2008.

[7] R. Dhamija and A. Perrig, "User Study Using Images for Authentication," in *Proceedings of USENFX Security Symposium*, 2000.

[8] K. Gilhooly, "Biometrics: Gctting Back to Business," in *computer world*, May 09, 2005.

[9] H. Gsworth and A. J. S. Flenderson, "Accurate visual memory for previously attended objects in natural scenes," *Journal of Experimental Psychology -Human Perception and Performance*, vol. 28, 2002, pp. 113-136

[10] Information security Breaches Survey 2006, Price Porterhouse Coopers, April 2006.

[11] S. Madigan and J. C. Yuille, "Picture Memory, Ineditor, Imagery memory and cognition," pp. 65-89, *Lawrence Erlbaum Associates*, 1983.

[12] D. L. Nelson, U. S. Reed, and R. Allmg, "Picture superiority effecl," *Journal of Experimental Psychology: Human Learning and Memory*, vol. 3, 1977, pp. 485-497

[13] Passlogix. [Online]. Available: http:/Avww.passlogix.com

[14] L. D. Paulson, "Taking a Graphical Approach to the Password," *Computer*, vol. 35, pp. 19, 2002.

[15] Real User Corporation. The Science behind Passfaces. [Online]. Available: www.realuser.com/published/ScienceBehindPassfaces.pdf

[16] R. N. R. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163.

[17] Viskey. [Online]. Available: vww.viskey.com/tech.html

[18] R. N. Sheperd, "Recognitiontnemory for \vords,sentences and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp 156-163, 1967.

[19] L. P. Standing, "Learning 10,000 pictures quarterly," *Journal of Experimental Psychology*, vol. 25, pp. 207-222.

[20] S. Wiedenbeck. J. Waters, J. C. Birget, A. Brodskiy, and N. Menon, "Authentication using graphical pass\vords: Basic results," In *Human-Computer Interaction International (HCII 2005)*, Las Vegas, NV, 2005.

[21] S. J. W. Beck, C. Birget, A. Brodskiy, and N. Menon, "Authentication using graphical passwords: Effects of tolerance and image choice," In *Symposium on Usable Privacy and Security (SOUPS)*, Carnegie-Mellon University, Pittsburgh 2005.

[22] S. J. W. Beck, C. Birget, A. Brodskiy, and N. Menon, Pass Points: "Design and longitudinal evaluation of a graphical,"

P. Rama Bayapa Reddy completed BE in computers from Marathwada University ,Aurangabad and M.Tech from JNTU, Anantapur. Now presently pursuing Ph.D from JNTUA, Anantapur. My interested Research area is internet controlled embedded systems.I conducted two national level seminars I am working as Professor in Computer Science and Engineering in Dhruva institute of Engineering and Technology, Hyderabad. putluru.ramreddy@gmail.com

K. Soundararajan received the B.E Degree in Electronics and Communications from S.V.U, Tirupati and M.Tech Degree in Instrumentation and control Engg. from J.N.T.U, Kakinada. Presently, he is working as Professor, Department of ECE, JNTUACE, of Jawaharlal Nehru Technological University College of Engineering, Anantapur, A. P,India. soundararajan_jntucea@yahoo.com

M. H. M. Krishna Prasad has completed B.Tech, M.Tech (CSE), JNTU, Hyderabad Ph.D., in Computer Science & Engineering from JNTU Hyderabad Presently he is working as Associate Professor of CSE & Head, Dept. of Information Technology University College of Engineering JNTUK-Vizianagaram Campus, Vizianagaram, A.P, India.