International Journal of Electronic and Electrical Engineering.
ISSN 0974-2174 Volume 7, Number 8 (2014), pp. 837-841

http://www.irphouse.com

Enhancing Cloud Security By: Gotcha (Generating Panoptic Turing Tests to Tell Computers and Human Aparts)

Pawan Gupta[1] and Mohd. Suhail Ansari[2]

[1]Student at Dept. of Information Technology,
University of petroleum and energy studies, Dehradun, Uttrakhand
[2]Student at Dept. of Material Science and Nano Technology,
University of petroleum and energy studies, Dehradun Uttrakhand.

ABSTRACT

Cloud computing is the starting of a new era in IT Industry, Cloud computing is the delivery of computing components as a service. Today almost every IT company and different sectors such as Health, Tourism, fishing and government of different countries are making huge investment in cloud computing. On an average, by 2018, government sector will invest $18. 48 Billion, health sector will invest $5. 4 Billion, IT giants like IBM and CISCO will invest $2 to $3 Billion on cloud computing. But one of the biggest challenges faced by this technology is SECURITY. Today Cyber-crime has strengthened its routes, as a result there are security breaches raised in network security. To mitigate the risk of hacking and enhancing cloud security GOTCHA (Generating panoptic Turing Tests to Tell Computers and Humans Apart) is introduced as a way of preventing automated offline dictionary attacks against user selected passwords. A GOTCHA is a randomized puzzle generation protocol, which involves interaction between a computer and a human. Informally, a GOTCHA should satisfy two key properties:

(1) The puzzles are easy for the human to solve.
(2) The puzzles are hard for a computer to solve even if it has the random bits used by the computer to generate the final puzzle unlike a CAPTCHA. GOTCHAs can be used to mitigate the threat of offline dictionary attacks against passwords by ensuring that a password cracker must receive constant feedback from a human being while mounting an attack. GOTCHA relies on the usability assumption that users can recognize the phrases that they originally used to describe each Inkblot image a much weaker usability assumption than previous password systems based on Inkblots which required users to recall their phrase exactly.

KEYWORD: Security breaches, offline dictionary attack, protocol, mounting.

1. INTRODUCTION

Cloud computing portends a major change in how we store information and run applications. Instead of running pro-grams and data on an individual desktop computer, every-thing is hosted in the "cloud"—a nebulous assemblage of computers and servers accessed via the Internet. Cloud computing lets you access all your applications and documents from anywhere in the world, freeing you from the confines of the desktop and making it easier for group members in different locations to collaborate. . Clouds are a large pool of easily usable and accessible virtualized resources such as hardware, development platforms and services can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of pay-per-use for resources model with guaranties from Infrastructure Provider by means of customized Service Level Agreements. But as per the threats to cloud security are increasing, user's data can be compromised as any person who has obtained the cryptographic hash of a user's password can mount an automated brute-force attack to crack the password by comparing the cryptographic hash of the user's password with the cryptographic hashes of likely password guesses. This attack is called an offline dictionary attack, and there are many password crackers that a person can use. Servers have been compromised at large companies (Facebook, LinkedIn, Sony etc.) resulting in the release of millions of cryptographic password hashes. It has been repeatedly demonstrated that users tend to select easily guessable passwords and password crackers are able to quickly break many of these passwords. Offline attacks are becoming increasingly dangerous as computing hardware improves a modern GPU can evaluate a cryptographic hash function like SHA2 about 250 million times per second and as more and more training data leaked passwords from prior breaches becomes available.

2. Literature Review

Concept of cloud computing started back to the 1950s, when large-scale mainframe computing comes into existence. Since 2000, Amazon played a key role in the development of cloud computing by modernizing their data centers. Amazon initiated a new product development provide cloud computing to external customers, and launched Amazon Web services (AWS) on the basis of Utility Computing. In 2011, IBM announced the IBM Smart Cloud framework to support Smarter Planet Initiative. CAPTCHAs were introduced in 2000 by Luis von Ahn and pals at Carnegie Mellon University in Pittsburgh. Hermann Rorschach is the Swiss psychologist who invented the inkblot-based personality tests. GOTCHA was also used to counteract hackers that breach the walls of a server to download lists of user names and passwords. The likes of Zappos (2012), LinkedIn (2012), Sony (2011), and Gawker (2010) have all been hit, inspiring a search for a better security system.

3. HOSP (Human Only Solvable Puzzles)

HOSP are randomized puzzles like CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart) which are generated by the servers

to determine whether or not the user is human. CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as a reverse Turing test. CAPTCHAs can prevent bot-generated spam by requiring that the (unrecognized) sender pass a CAPTCHA test before the email message is delivered, but the technology can also be exploited by spammers by impeding OCR detection of spam in images attached to email messages. CAPTCHAs have also been used to prevent people from using bots to assist with massive downloading of content from multimedia websites. They are used in online message boards and blog comments to prevent bots from posting spam links as a comment or message. There are certain Drawbacks of HOSP - Techniques have been built which can beat CAPTCHAs with 99. 8 percent accuracy (e. g. OCR (optical character recognition)) which are mature enough to beat CAPTCHAs.

4. GOTCHA

Inkblots have been proposed as an alternative way to generate and remember passwords. It is proposed to show the user ten randomly generated inkblot images and having the user make up a word or a phrase to describe each image. It is stressed that the use of Inkblot images is different in two ways:

(1) Usability: It is not required for users to recall the word or phrase associated with each Inkblot. Instead it is required for user's to recognize the word or phrase associated with each Inkblot so that they can match each phrase with the appropriate Inkblot image. Recognition is widely accepted to be easier than the task of recall.
(2) Security: It is not needed to assume that it would be difficult for other humans to match the phrases with each Inkblot. But it is assumed that it is difficult for a computer to perform this matching automatically.
(3) Timer: A timer can also be set within the GOTCHA to mitigate offline dictionary attacks e. g. if a brute force attack is used to crack the password, after an attempt of 5 unmatched passwords a new GOTCHA should appear which should be quite difficult then the before Inkblot image.

To create a GOTCHA, user chooses a password and a computer then generates several random, multi-colored inkblots. User describes each inkblot with a text phrase, and these phrases are stored in random order along with the password. When user return to the site and sign in with the password, the inkblots are displayed again along with the list of descriptive phrases. You then match each phrase with its corresponding inkblot.

5. HOSP (Human Only Solvable Puzzles) vs. GOTCHA

HOSPs (Human Only Solvable Puzzles) is a way of defending against offline dictionary attacks. The basic idea is to change the authentication protocol so that

human interaction is required to verify a password guess. The authentication protocol begins with the user entering his password. In response the server randomly generates a challenge using the password as a source of randomness for the user to solve. Finally, the server appends the user's response to the user's password, and verifies that the hash matches the record on the server.

There is a simple modification of HOSPs that are called GOTCHAs (Generating panoptic Turing Tests to Tell Computers and Humans Apart). The adjective Panoptic is used to refer to a world without privacy there are no hidden random inputs to the puzzle generation protocol. The basic goal of GOTCHAs is similar to the goal of HOSPs defending against offline dictionary attacks. GOTCHAs differ from HOSPs in two ways:

(1) Opposing a HOSP a GOTCHA may require human interaction during the generation of the challenge.
(2) Relaxation is given in the requirement that a user needs to be able to answer all challenges easily and consistently.

If the user can remember his password during the authentication protocol then he will only ever see one challenge. It only requires that the user must be able to answer this challenge consistently. If the user enters the wrong password during authentication then the user may see new challenges. We do require that it is difficult for a computer to distinguish between the "correct" challenge and an "incorrect" challenge. This paper demonstrates that GOTCHAs like HOSPs can be used to defend against offline dictionary attacks. The goal of these relaxations is to enable the design of usable GOTCHAs. GOTCHAs are based on inkblot images. While the images are generated randomly by a computer, the human mind can easily imagine semantically meaningful objects in each image. To generate a challenge the computer first generates ten inkblot images. The user then provides labels for each image (e. g. , evil clown, big frog). During authentication the challenge is to match each inkblot image with the corresponding label.

6. CONCLUSION AND FUTURE SCOPE

GOTCHAs can be widely used to increase the cloud security because GOTCHAs allow for human feed- back during puzzle generation unlike HOSPs which potentially opens up a much wider space of potential GOTCHA constructions.

One idea might be to have a user rate/rank random items (e. g. , movies, activities, foods). By allowing human feedback we could allow the user to dismiss potentially confusing items (e. g. , movies he hasn't seen, foods about which he has no strong opinion).

Interaction is an incredibly powerful tool in computer security, human authentication typically does not exploit interaction with the human (e. g. , the user simply enters his password).

We view the idea behind HOSPs and GOTCHAs exploiting interaction to mitigate the threat of offline attacks as a positive step in this direction.

GOTCHAs can not only be used to improve cloud security but can also be used to create more secure networks and help the cyber world in mitigating the risk of cyber-crime.

7. REFERENCE

[1] MARK VANDERWIELE, "The IBM Research Cloud Computing Initiative", Keynote talk at ICVCI 2008, RTP, NC, USA, 15–16 May 2008.
[2] Beak, R. Safavi-Naini, and W. Susilo. Public key encryption with keyword search revisited. In International conference on Computational Science and Its Applications, pages 1249-1259. Springer-Verlag, 2008.
[3] Baek, R. Safavi-Naini, and W. Susilo. Public key encryption with keyword search revisited. In International conference on Computational Science and Its Applications, pages 1249-1259. Springer-Verlag, 2008.
[4] D. Song, D. Wagner, and A. Perrig. Practical techniques for searching on encrypted data. In IEEE
[5] Symposium on Research in Security and Privacy, pages 44-55. IEEE Computer Society, 2000.
[6] Luis M. Vaquero,Luis Rodero-Merino, Jua critical areas of focus in cloud computing. Technical report, Cloud Security Alliance, April 2009.
[7] Luis M. Vaquero, Luis Rodero-Merino, Jua critical areas of focus in cloud computing. Technical report, Cloud Security Alliance, April 2009.
[8] A. Shamir. Ip= pspace. Journal of the ACM (JACM), 39(4):869–877, 1992.