A PROBABILISTIC MODEL OF VISUAL CRYPTOGRAPHY SCHEME FOR ANTI-PHISHING

M.Kavitha[1], P.Thanigesan[2]
[1,2]Computer Science and Engineering, Indira Institute of Engineering and Technology, Chennai, India

Abstract

Cell discontinuous transmission (DTX) has been proposed as a solution to reduce the energy consumption of cellular networks. This paper investigates the impact of network traffic load on the spectral and energy efficiency of cellular networks with DTX. The signal-to-interference-plus-noise ratio (SINR) distribution as a function of traffic load is derived first. Then, the sufficient condition for ignoring thermal noise and simplifying the SINR distribution is investigated. Based on the simplified SINR distribution, the network spectral and energy efficiency as functions of network traffic load are derived. It is shown that the network spectral efficiency increases monotonically in traffic load, while the optimal network energy efficiency depends on the ratio of the sleep-mode power consumption to the active-mode power consumption of base stations. If the ratio is larger than a certain threshold, the network energy efficiency increases monotonically with network traffic load and is maximized when the network is fully loaded. Otherwise, the network energy efficiency first increases and then decreases in network traffic load. The optimal load can be identified with a binary search algorithm. The power ratio threshold depends solely on the path loss exponent α, e.g., 56% for α = 4. All these analytic results are further validated by the numerical simulations.

INTRODUCTION

OUTLINE OFTHE PROJECT

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective.

Thus the security in these cases be very high and should not be easily tractable with implementation easiness. Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem.

As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not. Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security.

phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication.

one definition of phishing is given as “it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication”. The conduct of identity theft with this acquired sensitive information has also become easier with the use of technology and identity theft can be described as “a crime in which the impostor obtains key pieces of information such as Social Security and driver's

license numbers and uses them for his or her own gain". Phishing attacks rely upon a mix of technical deceit and social engineering practices. In the majority of cases the phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information.

Communication channels such as email, webpages, IRC and instant messaging services are popular. In all cases the phisher must impersonate a trusted source for the victim to believe. To date, the most successful phishing attacks have been initiated by email – where the phisher impersonates the sending authority

So here introduces a new method which can be used as a safe way against phishing which is named as "A novel approach against Anti-phishing using visual cryptography". As the name describes, in this approach website cross verifies its own identity and proves that it is a genuine website (to use bank transaction, E-commerce and online booking system etc.) before the end users and make the both the sides of the system secure as well as an authenticated one. The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a method of encrypting a secret image to shares, such that stacking a sufficient number of shares reveals the secret image.

Problem Definition

Online transactions are nowadays become very common and there are various attacks present behind this. In these types of various attacks, phishing is identified as a major security threat and new innovative ideas are arising with this in each second so preventive mechanism should also be so effective.

Thus the security in these cases be very high and should not be easily tractable with implementation easiness.

Today, most applications are only as secure as their underlying system. Since the design and technology of middleware has improved steadily, their detection is a difficult problem.

As a result, it is nearly impossible to be sure whether a computer that is connected to the internet can be considered trustworthy and secure or not.

Phishing scams are also becoming a problem for online banking and e-commerce users. The question is how to handle applications that require a high level of security.

Objective

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication.

One definition of phishing is given as "it is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication".

So here introduces a new method which can be used as a safe way against phishing which is named as " On the Relation of Random Grid and Deterministic Visual Cryptography". As the name describes, in this approach website cross verifies its own identity and proves that it is a genuine website (to use bank transaction, E-commerce and online booking system etc.) before the end users and make the both the sides of the system secure as well as an authenticated one. The concept of image processing and an improved visual cryptography is used. Image processing is a technique of processing an input image and to get the output as either improved form of the same image and/or characteristics of the input image. Visual Cryptography (VC) is a method of encrypting a secret image to shares, such that stacking a sufficient number of shares reveals the secret image.

ALGORITHMS:

GRAYSCALE CONVERSION:

The Captcha image first converts into grayscale using luminance method.

LUMINOSITY:

The gray level will be calculated as

Luminosity = $0.21 \times R + 0.72 \times G + 0.07 \times B$

VCS SCHEME:

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub

pixels called shares... Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices.

When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

RANDOM NUMBER:

- Java includes a wealth of functions that you can use in your programs. However, Java runs with a minimal amount of functions already available. This helps with processing time and saves extra lines of code. When you want to use a certain feature, such as receiving input from the user or generating a random number, you need to import that utility into your code. We use the import statement to do this. The tool we'll be using is the Random class, which is part of Java's utility (util) library.
- We can generate random number using rand object. We should provide some seeding to rand object so that the number generated are different. If we does not provide the seeding then the compiler always produce the same result.
- Import java.util.Random;
- We will need to set our limits; in this case we only want a number between 1 and 100. Let's create two integer variables for this purpose, like this:
- Int max=100;
- Int min=0;
- Next we can setup the actual random number generator. Random is a class in Java, with its own methods. We can create an instance of this class and use all of these cool features. In order to create a new instance of Random, this code is used
- Finally, we can generate our random number. The Random class provides a method called nextInt(int n), which generates a random number between 0 and the number specified (n). We want only numbers between 1 and 100, so the code is tweaked a little bit. It may look a little confusing, but we'll walk through it. Here is the code to generate a random number between 1 and 100 and save it to a new integer, showMe:

```
int showMe = min + randomNum.nextInt(max);
```

Each time we run the program a different number is displayed between 1 and 100. Here is the final, complete code:

```
public static void main(String[] args) {

 //what is our range?
 int max = 100;
 int min = 1;

 //create instance of Random class
 Random randomNum = new Random();

 int showMe = min + randomNum.nextInt(max);
 System.out.println(showMe);

}
```

Modules

- Registration With Secrete Code
- Image captcha Generation
- Shares Creation(VCS)
- Login Phase

Module Description

Registration With Secrete Code:

In the registration phase, the user details user name,password,email-id,address,and a key string(password) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure environment. This string is concatenated with randomly generated string in the server.

Image captcha Generation:

A key string is converted into image using java classes BufferedImage and Graphics2D. The image dimension is 260*60.Text color is red and the backround color is white.Text font is set by Font class in java.After image generation it will be write into the userkey folder in the server using ImageIO class.

Shares Creation(VCS):

The image captcha is divided into two shares such that one of the share is kept with the user and the other share is kept in the server. The user's share and the original image captchais sent

to the user for later verification during login phase. The image captcha is also stored in the actual database of any confidential website as confidential data.

Login Phase:

When the user logs in by entering his confidential information for using his account, then first the user is asked to enter his username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the website for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user.

Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website.

Product Perspective

This product is combination of our main components, namely Image processing and visual cryptography, the web portal, web services and the JEE application. The main objective is predicting the phishing sites based on visual cryptography.

Implementation

NETBEANS IDE 7.0.1

The java code has been written in a easy to use "NetBeansIDE":which is a reusable framework for simplifying the development of other desktop applications. When an application based on the NetBeans Platform is run, the platform's Main class is executed. Available modules are located, placed in an in-memory registry, and the modules' startup tasks are executed. Generally, a module's code is loaded into memory only as it is needed. Applications can install modules dynamically. Any application can include the Update Center module to allow users of the application to download digitally signed upgrades and new features directly into the running application. Reinstalling an upgrade or a new release does not force users to download the entire application again.

WORDNET

WordNet is a lexical database for the English language. It groups English words into sets of synonyms called synsets, provides short, general definitions, and records the various semantic relations between these synonym sets. The purpose is twofold: to produce a combination of dictionary and thesaurus that is more intuitively usable, and to support automatic text analysis and artificial intelligence applications. The database and software tools have been released under a BSD style license and can be downloaded and used freely. The database can also be browsed online.

The main relation among words in WordNet is synonymy, as between the words shut and close or car and automobile. Synonyms--words that denote the same concept and are interchangeable in many contexts--are grouped into unordered sets (synsets). Each of WordNet's 117 000 synsets is linked to other synsets by means of a small number of "conceptual relations." Additionally, a synset contains a brief definition ("gloss") and, in most cases, one or more short sentences illustrating the use of the synset members. Word forms with several distinct meanings are represented in as many distinct synsets. Thus, each form-meaning pair in WordNet is unique.

MySQL

The MySQL development project has made its source code available under the terms of the GNU General Public License, as Well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Sitdish company MySQL AB, now owned by Oracle Corporation. MySQL is a popular choice of database for use in We applications, and is a central component of the widely used LAMP open source We application software stack—LAMP is an acronym for "Linux, Apache, MySQL, Perl/PHP/Python". MySQL is an open source database management system and is used in some of the most frequently visited Websites on the Internet, including Flickr, Nokia.com, YouTube and as previously mentioned,Wikipedia, Google, Facebook and Twitter. MySQL is written in C and C++. Its SQL parser is written in yacc, and a home-brewed lexical analyzer named sql_lex.cc.MySQL works on many different system platforms,including AIX, BSDi,

FreeBSD, HPUX, eComStation, i5/OS, IRIX, Linux , MacOSX, MicrosoftWindows, NetBSD, Novell ,NetWare, OpenBSD, OpenSolaris, OS/2Warp, QNX, Solaris, Symbian, SunOS, SCO OpenServer, SCO UnixWare, Sanos and Tru64. A port of MySQL to OpenVMS also exists.

- The best and the most-used database in the world for online applications
- Available and affordable for all
- Easy to use
- Continuously improved while remaining fast, secure and reliable
- Fun to use and improve
- Free from bugs
- Subscribe to the Open Source philosophy
- Aim to be good citizens
- Prefer partners that share our values and mindset
- Answer email and give assistance to users, customers, partners and co-workers
- Be a virtual organization, networking with others

SQLyog:

SQLyog v0.9 was first released to the public in 2001 as closed source free software after eight months of development. SQLyog was freely available until v3.0 when it was made commercial software. SQLyog is available in free as well as paid versions. The free version is known as Community Edition and is available as an open source projectat Google Code. Paid version is sold as Professional, Enterprise and Ultimate Editions.

 Tabbed interface for connections. Connections can be given a color for identification.
 Editor with syntax highlighting and various automatic formatting options.
 Intelligent Code Completion.
 Data manipulations (INSERT, UPDATE, and DELETE) may be done from a spreadsheet-like interface. Both raw table data and a result set from a query can be manipulated.
 Rich context menus etc. for performing common tasks without writing SQL.
 Visual Schema Designer.
 Visual Query Builder.
 Query Formatter.
 Connectivity options: Direct client/server using MySQL API (SSL supported), HTTP/HTTPs Tunneling, SSH Tunneling.
 Wizard driven Tool for import of data from ODBC-databases
 Backup Tool for performing unattended backups. Backups may be compressed and optionally stored as a file-per-table as well as identified with a timestamp.
 'SQL Scheduler and Reporting Tool' - a tool for scheduling and automating execution of any sequence of SQL statements. Result of queries may be sent as HTML-formatted reports.

Tomcat Server:

Tomcat is an open source web server developed by Apache Group. Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies. The Java Servlet and JavaServer Pages specifications are developed by Sun under the Java Community Process. Web Servers like Apache Tomcat support only web components while an application server supports web components as well as business components (BEAs Weblogic, is one of the popular application server).To develop a web application with jsp/servlet install any web server like JRun, Tomcat etc to run your application.

A Web server handles the HTTP protocol. When the Web server receives an HTTP request, it responds with an HTTP response, such as sending back an HTML page. To process a request, a Web server may respond with a static HTML page or image, send or redirect, or delegate the dynamic response generation to some other program such as CGI scripts, JSPs (JavaServer Pages), servlets, ASPs (Active Server Pages), server-side JavaScripts, or some other server-side technology. The web server simply passes the request to the program to handle it. The web server does not provides any functionality beyond providing an environment in which the server - side program can execute and pass back the generated responses. The server-side program usually provides such functions as transaction processing, database connectivity and messing.

While an application server exposes business logic to client applications through various protocols like HTTP, TCP-IP etc. All the web servers mainly deals with sending HTML for displaying to a Web browser. An application

server providers allows the client to access the business logic for use. The application server is used to run business logic or dynamically generating presentation code. A J2EE application server runs servlets and JSPs that are used to create HTML pages dynamically. In this case, J2EE application server can run EJBs ?which are used to execute business logic. An application server is more capable of dynamic behaviour than webserver.

SOFTWARE OVERVIEW

Java is a platform Independent. Java is a high level programming language Introduced by Sun Microsystems in June 1995 Java is becoming a standard for Internet Applications. It provides for interactive processing and for the use of graphics and animation on the Internet. Since the Internet consists of different types of computers and operating systems, a common language was needed to enable computers to run programs that run on multiple platforms. Java is an object-oriented language built upon C and C++.It derives its syntax from C and its object-oriented features are influenced by C++. Java can be used to create applications and applets. An application is a program that runs on the user's computer, under its operating system. An applet is a small window based program that runs on HTML page using Java enabled We browser like Internet Explorer, Netscape Navigator, HotJava or an applet view

3.3.2 FEATURES OF JAVA:

- Simple
- Object Oriented
- Platform Independent
- Robust
- Secure
- Distributed
- Multithreaded
- Dynamic

SYSTEM IMPLEMENTATION

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and effective. It may be implementation of a modified application to replace an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system.

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly.

Initially as a first step the executable form of the application is to be created and loaded in the common server machine which is accessible to the entire user and the server is to be connected to a network. The final stage is to document the entire system which provides components and the operating procedures of the system. Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Implementation is the process of converting a new system design into operation. It is the phase that focuses on user training, site preparation and file conversion for installing a candidate system. The important factor that should be considered here is that the conversion should not disrupt the functioning of the organization

CONCLUSION

Currently phishing attacks are so common because it can attack globally and capture and store the users' confidential information. This information is used by the attackers which are indirectly involved in the phishing process. Phishing websites as well as human users can be easily identified using our proposed "Anti-phishing framework based on VisualCryptography". The proposed methodology preserves confidential information of users. Verifies whether the website is a genuine/secure website or a phishing website. If the website is a phishing website (website that is a fake one just similar to secure website but not the secure website), then in that situation, the phishing website can't display the image captcha for that specific user (who wants to log in into the website) due to the fact that the image

captcha is generated by the stacking of two shares, one with the user and the other with the actual database of the website. The proposed methodology is also useful to prevent the attacks of phishing websites on financial web portal, banking portal, online shopping market.

References

- R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Comput. Surveys*, vol. 44, no. 4, 2012.
- (2012, Feb.). *The Science BehindPassfaces*[Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf
- Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in *Proc. 8th USENIX Security Symp.*, 1999, pp. 1–15.
- H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," *Int. J. Netw. Security*, vol. 7, no. 2, pp. 273–292, 2008.
- S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *Int. J. HCI*, vol. 63, pp. 102–127, Jul. 2005.
- P. C. van Oorschot and J. Thorpe, "On predictive models and userdrawn graphical passwords," *ACM Trans. Inf. Syst. Security*, vol. 10, no. 4, pp. 1–33, 2008.
- K. Golofit, "Click passwords under investigation," in *Proc. ESORICS*, 2007, pp. 343–358.
- E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in Proc. Symp. Usable Privacy Security, 2007, pp. 20–28.
- J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hot spots in graphical passwords," in *Proc. USENIX Security*, 2007, pp. 103–118.
- P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on passpoints-style graphical passwords," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 393–405, Sep. 2010.
- P. C. van Oorschot and J. Thorpe, "Exploiting predictability in clickbased graphical passwords," *J. Comput. Security*, vol. 19, no. 4, pp. 669–702, 2011.
- T. Wolverton. (2002, Mar. 26). *Hackers Attack eBay Accounts* [Online]. Available: http://www.zdnet.co.uk/news/networking/2002/03/ 26/hackers-attack-ebay-accounts-2107350/
- HP TippingPointDVLabs, Vienna, Austria. (2010). *Top Cyber Security Risks Report, SANS Institute and Qualys Research Labs* [Online]. Available: http://dvlabs.tippingpoint.com/toprisks2010
- Pinkas and T. Sander, "Securing passwords against dictionary attacks," in Proc. ACM CCS, 2002, pp. 161–170.