Middle-East Journal of Scientific Research 24 (S1): 388-392, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.S1.74

NextG Privacy [NP]-An Armament against Cyber Attacks

[1]S.A. Srinivasan and [2]V. Kavitha

[1,2]Department of Computer Science and Engineering,
Sri Sairam Engineering College, Chennai, Tamil Nadu, India
[2] Research Scholar SCSVMV University, India

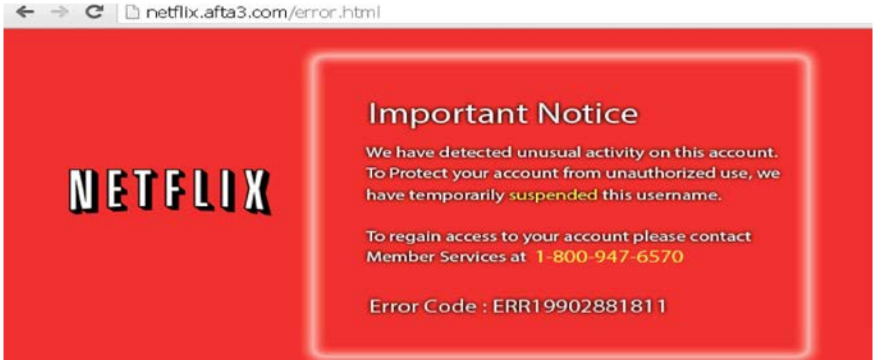
Abstract: Phishing is the attempt to acquire sensitive information such as user name, password and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. By introducing a dynamic-grid of security image followed by a caption during sign-in process, users can easily identify malicious entities and also overcome targeted phishing attacks. The proposed system then prompts for a user-interactive CAPTCHA which identifies whether the user is a person or malicious entity, thus overcoming Malware attacks. After signing in, the user credential will be encrypted using the proposed NPIN protocol, which generates a numeric version of the entered string and adds padding with random letters using Magic Square. The encrypted data will then be hidden inside an image using bit manipulation, making it invisible for Man-in-the-middle attacks.

Key words: Phishing · Dynamic-Grid · Overcome targeted phishing attacks · Catcher · Encrypted data · Next Privacy · NPIN protocol · MITM(Man-in-the-middle) attacks.

INTRODUCTION

The mainstay of the project is to provide a secured authentication mechanism by protecting the user from commonly encountered attacks like Phishing, Malware and MITM attacks. The Chosen String attack that can be done on RSA protocol is also addressed in this project [1]. Phishing attacks, also known as Ransom wares, have soared up by 113% in the past 2 years. Recently, users of the Internet Streaming Media giants, Netflix were the victims of a massive Phishing attack.

The conventional Man-in-the-middle Attack is also back on its feet again [2]. Still this type of attack constitutes 11.9% of the total cyber-attacks. Malwares like Game over Zeus and Crypto Locker are on circulation which attacks financial accounts.



netflix.afta3.com/error.html

NETFLIX

Important Notice

We have detected unusual activity on this account. To Protect your account from unauthorized use, we have temporarily suspended this username.

To regain access to your account please contact Member Services at 1-800-947-6570

Error Code : ERR19902881811

Fig. 1: Netflix Phishing Scam

In this project, an APPT is adopted, where dynamic grids of images are displayed, out of which the image closest to the user's secret category is selected and the caption provided is displayed [3]. This allows the user to easily identify malicious entities.

Corresponding Author: V. Kavitha, Research Scholar SCSVMV University, India.

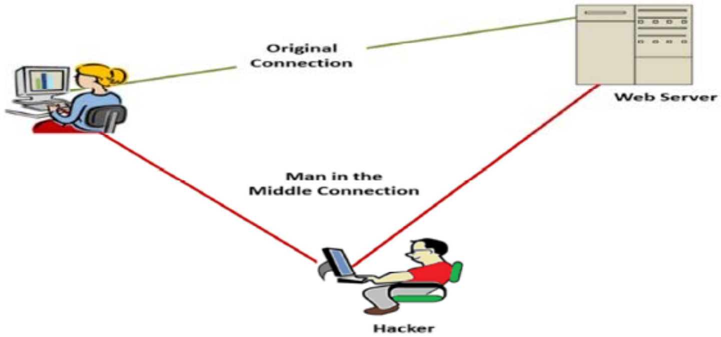
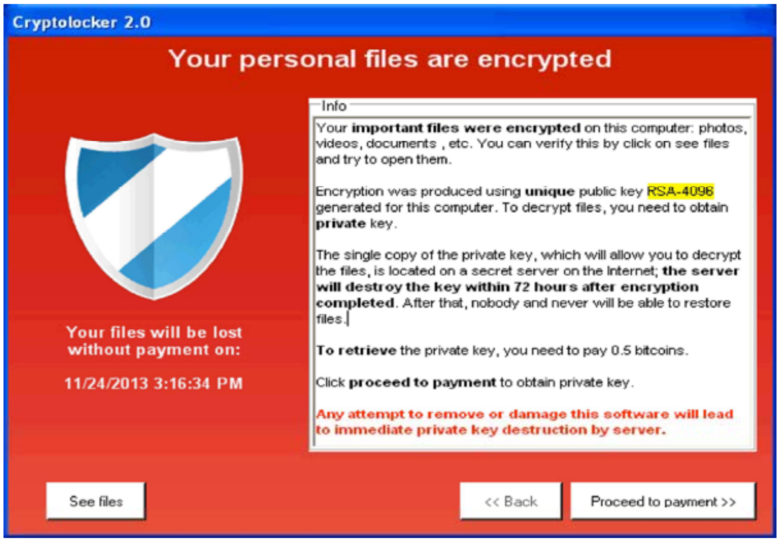


Fig. 2: MITM Atack

User Interactive CAPTCHA is then used to overcome the Malware attacks. Encryption of the data is done using the proposed NP protocol where an integer equivalent of the entered string is constructed and is padded with random letters using Magic square [4]. The encrypted data is then hid inside a PNG image, which overcomes the MITM attack. Thus, this project provides a completely safe authentication mechanism for the user. This work has great applications in Internet Banking and also in Social networks.



Your personal files are encrypted

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Fig. 3: Crypto Locker – Malware Attack

Related Work: [1] In "The Effectiveness of Security Images in Internet Banking"., Lee, J. Bauer, L. Mazurek and M.L. have analysed the effectiveness of static security image and caption that is currently being used in Internet Banking authentication system [5]. Their future work is to enhance the static security image based authentication mechanism, to be even more effective without annoying the user.

[2] In "MITM attack in LAN environment using payload matching"., Al Abri, D. has analysed how MITM attacks are generally carried out in a LAN based Environment by using payload matching [6]. His future work is to overcome this loophole in a LAN based environment by detecting the MITM attack.

[3] In "Modification in spatial, extraction from transform: A new approach for JPEG steganography"., Dervish Morphed Hussein, M. Mohave and M. have proposed a steganography technique where the data is hidden inside a JPEG image. Their Future work is to hide the data inside the JPEG image without distorting it.

Proposed System: The proposed system requires the user to select a category during the registration process and provide a caption for it. During the login process, a dynamic grid of images will be displayed and the user has to select the image that closely matches the secret category he chose. Upon Selection, the caption he provided will also be displayed. In addition to it, each user will be assigned a unique token (managed at the backend), which will be set in the user's browser as a cookie [7]. If that particular cookie is absent, an E-mail will be sent to the user where he needs to use the verification code to verify himself. Thus targeted phishing attack is impossible. User interactive CAPTCHA is used to distinguish between malware and user activity. The user data is then encrypted using NP protocol, where an integer equivalent to the string entered is constructed and is padded with random alphanumeric characters by using magic square. It then hides the encrypted data within the PNG image that is sent back to the backend.

Advantages:

- Targeted Phishing attacks can't be done since the attacker cannot know the user's secret image and caption unless and until his browser his verified. This makes it impossible for him to replicate the template.
- User interactive CAPTCHA can't be brute forced by malwares.
- Chosen String attack can't be done since the NP protocol generates totally random cipher text every time it encrypts the data.
- Since the encrypted data is inside a PNG image, it makes it invisible to the snoopers.

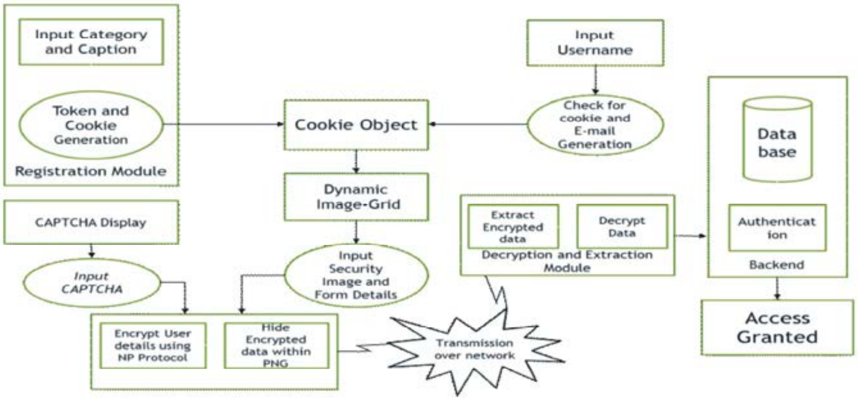
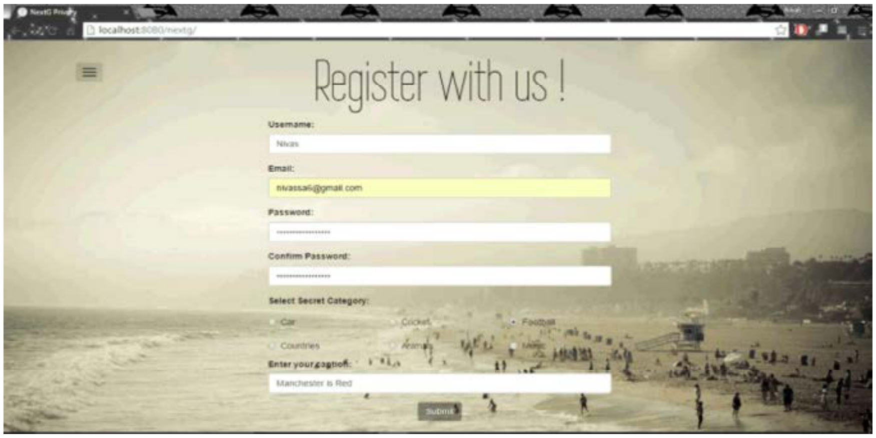

Input Category and Caption
Token and Cookie Generation
Registration Module
Cookie Object
Input Username
Check for cookie and E-mail Generation
Data base
Dynamic Image-Grid
CAPTCHA Display
Extract Encrypted data
Decrypt Data
Decryption and Extraction Module
Authentication
Backend
Input CAPTCHA
Input Security Image and Form Details
Access Granted
Encrypt User details using NP Protocol
Hide Encrypted data within PNG
Transmission over network

Fig. 4: Architecture Diagram

User Profile Setup: This module deals with setting up the user profile. During Registration process, the user has to choose a secret category from the list displayed and then provide a caption for it. After Registration is complete, a unique token is generated at the backend which is then added as cookie at the user's browser. Thus, this module makes it impossible for the attacker to collect user's secret information and caption information when it is a targeted attack. The attacker can get the user information only if his browser is verified as safe which is not possible unless he already has access to user's email account.



Register with us !

Username:
Nivas

Email:
nivassai@gmail.com

Password:
•••••••••••••••••

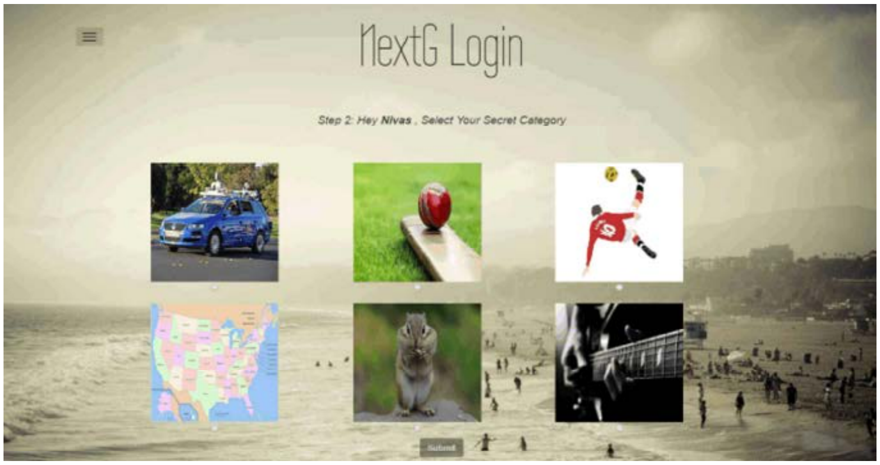
Confirm Password:
•••••••••••••••••

Select Secret Category:
○ Car ○ Cricket ● Football
○ Countries ○ Animals ○ Music

Enter your caption:
Manchester is Red

Fig. 5: User Profile Setup

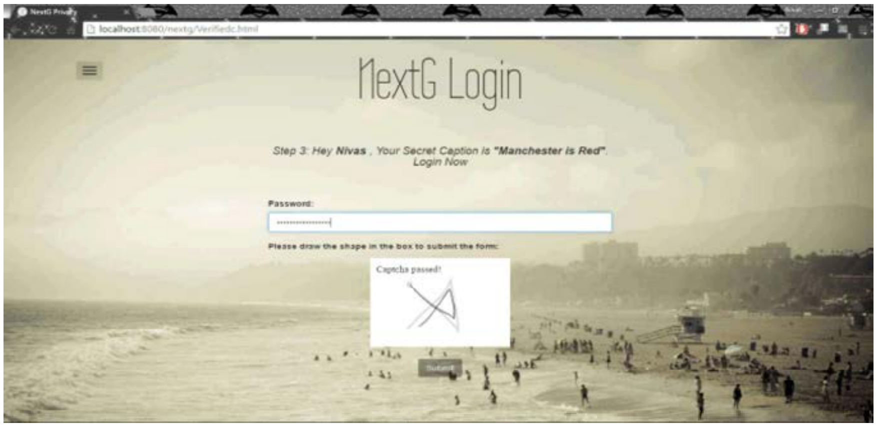
Dynamic Image-Grid and Cookie Verification: During the sign-in process, the cookie containing the user token is searched after the user enters his email-id. If the Cookie is found, a dynamic grid of image is displayed where one image closely matches with the user's secret category. If the cookie is not found, a verification code is generated which is sent to the user's email-id. Once the user selects the correct image and enters the correct verification code (if his browser is not verified), the caption provided by him will be displayed. This module allows the user to easily identify malicious entity and thus safeguards him from entering user credentials in unauthorized websites that mimics the original site.



Step 2: Hey **Nivas** , Select Your Secret Category

Fig. 6: Dynmic Grid of Images

Captcha Verification: Malwares can now brute force Text-Based CAPTCHA which voids the original purpose of fraud detection. This module introduces User-interactive CAPTCHA where the user has to draw the shape displayed on his screen. If the user's drawn shape hits 15 % of the original shape then the CAPTCHA is passed. Only if the CAPTCHA is passed, the user will be able to submit the form. This prevents malwares from brute forcing since it is 100% user activity.



localhost:8080/nextg/Verifiedc.html

Step 3: Hey **Nivas** , Your Secret Caption is **"Manchester is Red"**.
Login Now

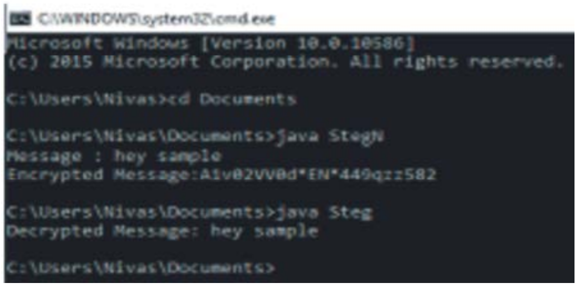
Password: ••••••••••••••••

Please draw the shape in the box to submit the form:

Captcha passed!

Fig. 7: CAPTCA verification

Data Encryption Using Np Protocol: Here an integer equivalent to the string entered is constructed by shifting the bits of a string 2 to the power 5 times, ensuring that a unique integer is constructed for every string and no collision happens. This Integer is then padded with random alphanumeric characters which is obtained from a 5x5 magic square. This way, a different cipher text is generated every time for the same string making it difficult for the attackers to do a chosen string attack.



```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Nivas>cd Documents

C:\Users\Nivas\Documents>java StegN
Message : hey sample
Encrypted Message:A1v02VV0d*EN*449qzz582

C:\Users\Nivas\Documents>java Steg
Decrypted Message: hey sample

C:\Users\Nivas\Documents>
```

Fig. 8: Sample Encryption and Decryption

Data Hiding Within Png Image: The encrypted data is then hid inside a PNG image without distorting it. This is done by taking unused pixels of the image, where each pixel is 8 bytes and Ending the last byte of image pixel and one character (1 byte) of the encrypted string. Simply put, least significant byte of the image represents one character of the encrypted string. Thus at the receiver's end, the least significant bytes of the unused pixels are extracted out to reform the original encrypted string. This module makes the encrypted data invisible for the snoopers. PNG images are used since it has the least overhead on the network traffic. Hiding data inside JPEG is not recommended since it has space-to-purpose efficiency of 1.3%. Encrypted string barely takes 1 kb while JPEG image will be more than 1 MB which is inefficient.

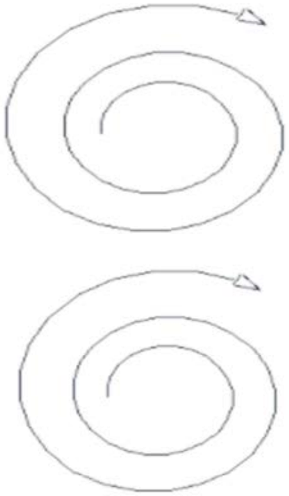


Fig. 9: Image before (top) and after (bottom) hiding data

Future Work: The Login process may annoy some users as its 3-step long. Thus, making it a one-step process by dynamically detecting cookies and sending emails will improve the login-time as well as good reception from the user side.

REFERENCES

1. Lee, J., L. Bauer and M.L. Mazurek, 2015. "The Effectiveness of Security Images in Internet Banking", Internet Computing, IEEE., 19(1), Issue Date: Jan. Feb. 2015).
2. Al Abri, D., 2015. "MITM attack in LAN environment using payload matching", Industrial Technology (ICIT), 2015 IEEE International Conference.
3. Darvish Morshedi Hosseini, M. and M. Mahdavi, 2015. "Modification in spatial, extraction from transform: A new approach for JPEG steganography", Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference.
4. Herley, C. and P.C. van Oorschot, 2012. "A research agenda acknowledging the persistence of passwords," IEEE Security and Privacy Magazine, 11(1): 28-36.
5. Bank of America, "Site Key FAQs," 2013. https://www.bankofamerica.com/privacy/faq/sitekey-faq.go, 2013.
6. PNC, 2013. "Online security information," https://www.pnc.com/webapp/unsec/Solutions.do?siteArea=/pnccorp/PNC/ Security+Information/ Security+Information, 2013.
7. Santander Bank, 2014. "SSA makes online banking even more secure," https://www.santanderbank.com/us/personal/banking/online-andmobile-banking/security-center/ssa-learn more, 2014.