STUDY OF PHISHING ATTACKS IN SOCIAL NETWORK

Muthu Palanivel.P.B
Computer Science & Engineering, Kalasalingam University, Srivilliputhur, India
muthupalanivel4@gmail.com

Vasanth Kumar.V
Computer Science & Engineering, Kalasalingam University, Srivilliputhur, India
viyavasanth@gmail.com

Ananda Krishnan. K
Computer Science & Engineering, Kalasalingam University, Srivilliputhur, India
kannanananda.k@gmail.com

NesaRani.A
Computer Science & Engineering, Kalasalingam University, Srivilliputhur, India
nesaraniabaraham84@gmail.com

Abstract— The phishing process mainly involves planning procedure in which the phishers decide which organization to be attacked, once they have planned they will setup a procedure for delivering the message and collecting the data. After the setup the attacker will attack with a phony message which appears to form a source. The last process will be collection of the information when the user enters into the phishing website and they use the information for committing the crime or fraud they will use the weakness of the software and security on both the server and client side for committing the fraud.

Keywords- Social Network; Phishing.

I. INTRODUCTION

Phishing is a mechanism or a process which is used for obtaining a secured information like username password, pin of a debit card and other secured information details which leads to the loss of money directly or indirectly. It can be done by making the user to enter his details into a website which is like the original website and takes all the personal secured information from the user. The main sources of Phishing are email spoofing and instant messaging. It is mainly used for cheating the users of a true website which results in the weakness of web security. The growing Phishing can be reduced by enforcing rules, providing user training, creating public awareness and educating the user not to use the same pattern of the passwords in all the websites.

Social Networking service is a platform which is used to build a various number of social networks which helps people to communicate with each other on various aspects like education employment opportunities etc. They allow various users or share ideologies on various aspects and photos, videos of various events and making others to know about activities which are happening in modern world who are in their network. The main process of social networking is to connect friends and establishing trust in between them. These services can be mainly split into three types, “socializing Social network services used for communicating with the existing friends, networking social network services used for non-social inter personal communication, Social navigation social network services used for helping users to find specific information or resources.”

In this process there will be a third party which will be an individual or a company who are in electronic communication. The main process is to trick the receivers about the details so that the attacker can gain the secured credentials which could be helpful for him to access the users accounts. There are many anti phishing measures proposed by many of the industrial practitioners by black listing various phishing website and products to make sure that the security will be easily provided to the users and to make sure that they are in a secured environment. The spam messages are also one of the most important causes of the phishing attack. The main life cycle of a phishing attack involves many process useful for gaining information from user. This steps include

- Planning
- Setup
- Attack
- Collection
- Fraud
- Post attack actions

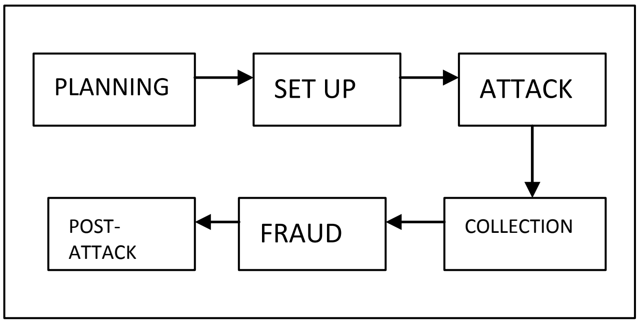


Figure 1.1: Steps in phishing

It is a process in which the attacker plans of attacking a certain organization or a target user. The target user will read the information setup by an attacker so that he can attacks a certain user. After the attack he collects all the data from the user so that he can use to make a fraud by taking all the details of the user.

II. PHISHING

Phishing is the process of stealing the personal and financial information of others. There are mainly two ways of phishing the first or common way is redirecting into malicious website like Typically a victim of the phishing process will receive a message or mail which will appears like it have been sent from a known user or an organization. When the victim opens the mail it consists of some links, images or attachment when these things are clicked once means then the victim will have redirected into a malicious page which setup to trick into giving of personal or financial information of the victim such as account ID, password details, credit card details, debit card pin or other information.

The another way is installing the malicious software to your system in this process the victim receives an attachment when the attachment is clicked the malicious software get installed and runs in the background of the system its main work is to collect the personal or financial information of the victim such as account ID, password details, credit card details, debit card pin or other information and sends it to the cyber criminals the victim will unaware of the malware which is running in background.

Phishing is the most popular cybercrime which is also famous among the cyber criminals it is also an easier trick when the malicious link is forwarded to the thousand victims means nearly 50% victims will fall in cyber theft.

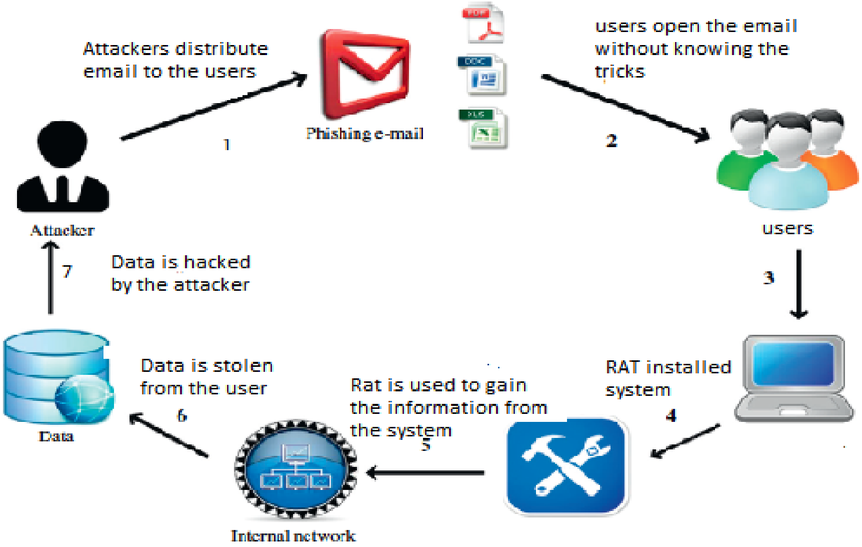

Attackers distribute email to the users
1
Phishing e-mail
users open the email without knowing the tricks
2
Attacker
users
7
Data is hacked by the attacker
3
Data is stolen from the user
6
Data
Rat is used to gain the information from the system
5
RAT installed system
4
Internal network

Figure 2.1: Phishing Attack

III. TECHNIQUES

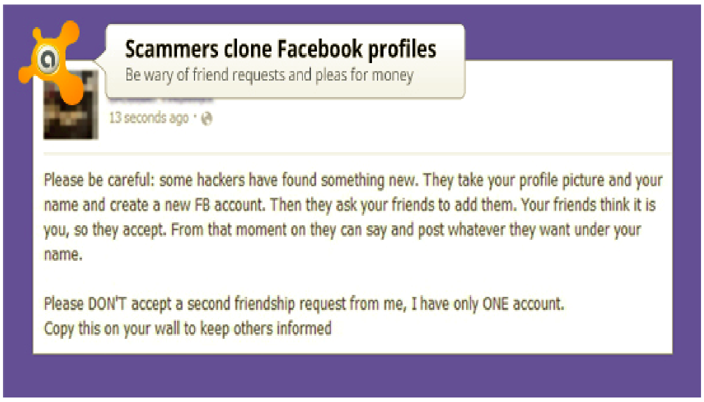
The main phishing techniques used by an attacker includes various process for deceiving the users. Some of them are explained below,

A. Spear Phishing:

The induguals or organizations that are directly affected by any of the phishing are generally come under a team known as Spear Phishing. In this the attacker will directly gather the secured personal information of the user to increase their rate of success. Normally through internet 91% of phishing attacks are taking place.

B. Clone Phishing:

In this procedure mainly the attacker concentrates on cloning the legitimate email send to a user which involves the attachment which can be replaced by a malicious link created by an attacker which appears to be coming from the original sender. Through this the attacker can get all the details of the user.



Scammers clone Facebook profiles

Be wary of friend requests and pleas for money

13 seconds ago

Please be careful: some hackers have found something new. They take your profile picture and your name and create a new FB account. Then they ask your friends to add them. Your friends think it is you, so they accept. From that moment on they can say and post whatever they want under your name.

Please DON'T accept a second friendship request from me, I have only ONE account.
Copy this on your wall to keep others informed

Figure 3.1: Clone phishing in Facebook profiles

C. Whaling:

Whaling is a process mainly used by the high level authorities like senior executives of an organization. This process mainly affects business emails forging the legitimate authorities and provides falsified companywide concern. Recently FBI subpoena emails gets attacked and special software is installed to monitor the Whaling attack.

D. Link Manipulation:

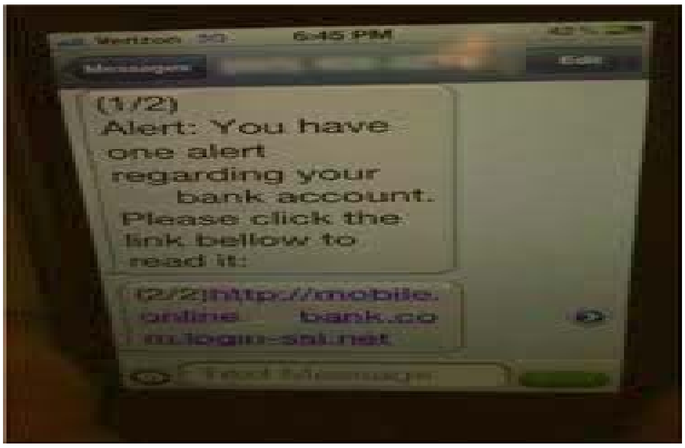
The main part of the manipulation includes the use of misspelled web link and the sub domains. Another trick by an attacker is to use a link which forged as a text to navigate a user to the phishers site. The another problem with URLs is the Internationalized Domain Name Spoofing using identical web addresses. The attackers easily get valid digital certificate to change content and spoof a genuine website.

E. Website Forgery:

The Phishing attacker's uses Java commands for manipulating the address bar. The original address bar image is hidden by the attacker and fake URL is created. The attacker uses some defects in a trusted website script and this type of attacks is particularly problematic when the user is directed to sign in at their bank webpage where the security certificate appears correct.

F. Phone Phishing:

In this type of phishing the attacker aims the victim and sends a message with the fake bank ID stating that there is a problem with their user account so as to send their phone number, after sending the phone number they will receive a message that they have successfully subscribed to a plan. In addition, stating that in order to deactivate proceed with the mentioned link. When the user proceeds with the link the user tends to fill the forum which results in giving their sensitive information. Thus the attacker gets the users sensitive details.



(1/2)
Alert: You have one alert regarding your bank account. Please click the link bellow to read it:

(2/2)http://mobile.online bank.com.login-ssl.net

Figure 3.2: Phone phishing

G. Web Spoofing:

The attacker creates a website which looks identical to the original website, the user fills the forum thinking that it is a genuine website. This results in the leakage of their personal information. Thus the attacker steals the information.

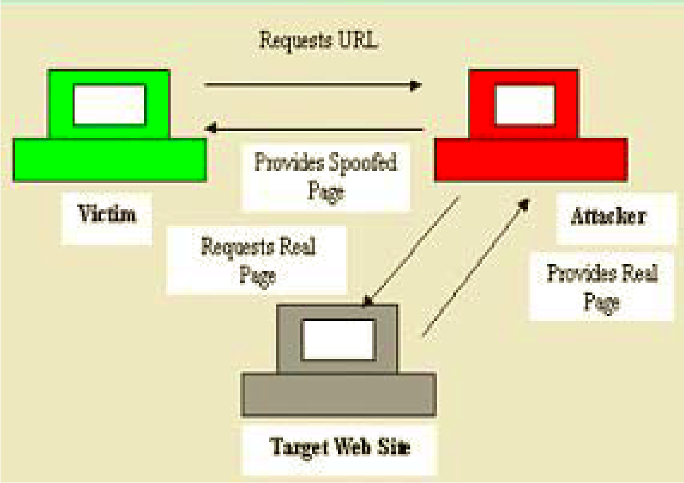


Figure 3.3: Web spoofing

H. Deceptive Phishing:

Deceptive Phishing is done by sending a message to the victim to confirm their information by sending the fake details, the user reenters their correct details. This is also done by giving fictitious account charges, modification in accounts and many other sites. The user tends to fill their details and they lose their personal information's.

I. Session Hijacking:

The Attacker will monitor the user until he/she open their account. Once they signed in to their account the malware software begins to perform and it makes transaction from their account without the victim's knowledge.

J. Data Theft:

The user information will be stored on the users Laptop/PC. The information such as credit card number, passwords, personal details, social security details, secret corporate information's is stolen by hearing secret conversations, legal opinions, secret documents, Company related documents. The thief sells this information to those who needs the destruction of the user.

IV. DETECTING A PHISHING EMAIL

A. Leak of images:

The images leaker by the hacker over the hacker over the network which the image of the user will never send over the network it will only displayed to the particular or personal user. To generate the image, the attacker must physically present to take or to capture the original image. It uses the extensive dictionary attack to capture the image it could not be used to take or reveal the password.

B. Man in middle attacks:

This is possible when an attacker act more intelligent during this process the attacker overlay the rogue windows over the trusted window or in browsers when the victim uses this window without any awareness he will fell into cyber thefts with the man in the middle in action and this types of attacks are very rare and very difficult for an attacker to execute.

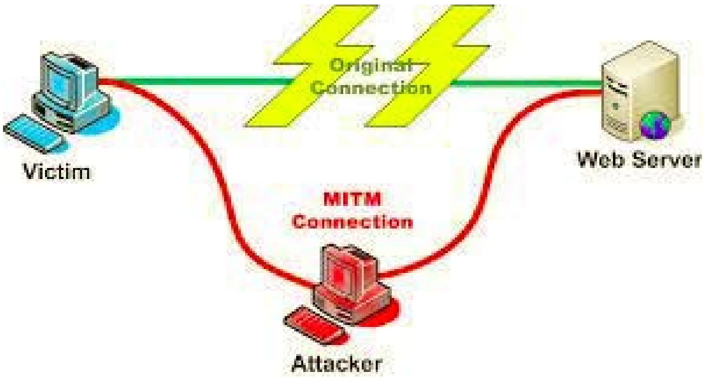


Figure 4.1: Man-In-The-Middle Attack

C. Spoofing the trusted window:

When the attacker has the minimum knowledge about the victim then it is easy to make the victim to trust the window these web pages provides the trusting environment to the users and the attacker gather the information like user ID, password and some personnel information.

D. spoofing the visual hashes:

It makes the phishers to make the visual hashes which show the web forms in a trusted website in a secure manner but it gives the information to the attacker by the process of visual hashes.

V. INTERACTIVE DESIGN AND INFORMAL TESTING

In this process they use the interactive designing process where the users are invited for informal tests in the process of informally interaction with mock-ups. The feedback gathered by this process will be used for the changes in the webpages and make a better prototype model. The previous version gives a random number to the user using the browser for every login but the user gets confused by this type of process provided by the browser to the server during SRP authentication. The user finds easy to recognize the image then the text which is used to create trusted path to the password window many user finds that the photographic image will provide a best password which also including their images user get more security however it can also weaken the security by tricking the user. The user has to gasp the concept of website by proving its identity by displaying the image by this process the user has able to match the images successfully to the website with their trusted window. The trusted window designs are tested for the acceptance and the resistance it provides against spoofing these windows are linked for the reorganization of the personal image the generated image must protected against the attacker where the image is generated and embedded but many of the users did not like the trusted window the design window must generally transparently visible underneath the personnel image Further design work is needed to optimize the size of the images to support the recognition and matching tasks, while minimizing the size of the window. We also need to determine the best format and placement for the window that supports current browsing behavior, interaction with trusted websites and that minimizes spoofing.

We adjusted the transparency of the images over the textboxes so that they maximized visibility of the image while minimizing interference with text entry. Some users expressed a desire to customize the placement of the textboxes, so that certain portions of the image are more visible.

VI. TWO STEP AUTHENTICATION

The two step verification process help the user to avoid the phishing process during the login process the dual step verification process provides the one-time password to the user number by using OTP the user can login securely to their page or account.

While clicking into the URL link check whether it is a correct link or not because the cyber criminals change one letter and create a fake look alike page for the phishing so the users must aware about the links while entering into it.

Always beware of Trojan malware which act like a software but it collects the user data and information and sends the information to the cyber criminals the user must always aware of Trojans because it will run in a background and provides the back door to the hackers.

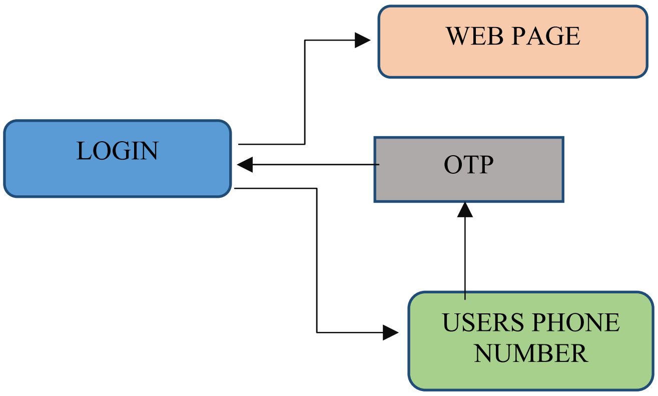


Figure 6.1: One Time Password (OTP) Method

VII. FORMAL EXPERIMENTAL USER STUDY DESIGN

The most of the evidence we have now the many spoofing and anti-spoofing techniques Provides some little data to this subject, the experimental study has the information of effectiveness of the image comparison and it will display some of the customization techniques using the remote servers. Now we are using the designing techniques to compare with designing and between subjects.

VIII. PROBLEMS

The loop pols in a security covers mainly three important areas at first Non uniformity of an internet standard will make easily to access the user data. The defective mail transferring system will also be useful for attackers to attack the secured information. The user's data transferring system will also play an important role in phishing attack.

The rapid growth process in phishing is also lead to the solutions about the phishing which has the number of proposed ranging for quick fix changes the anti-phishing properties includes the proposals to include the address and security.

The phishing problems can be divided into two approaches they are

A. Third party certification

These third party models include the public key infrastructure (pki) which has used for the authentication process and vice versa.

B. Direct authentication:

i Multi-factor user authentication.
ii AQL passcode.
iii Secondary SMS passwords.
iv Server authentication using shared secrets.
v Pass mark and verified by visa.

IX. SOLUTIONS FOR PHISHING ATTACK

A. Technical solution:

The URL which contain IP address must be taken in account. The IP address which are out of the range or out of parameter must be blocked. The bounced email messages must be monitored.

B. Policy changes:

The obvious deep domain names must be registered. The process must be language independent it must detect spam of any file type. The adaptive technology must be implemented for detecting the spammers constantly.

C. Heuristic Fraud Detection:

Mail secure concept uses the heuristic rules in order to detect possible phishing attacks.

D. Zombie Detection:

The attackers use zombie computers for distributing their mails.

E. IP Reputation:

This is the process used for blocking the zombie attack on the network which is based on the sniffers located at various points. This process technically classifies the IP address according to the profiles they built on like volumes % of spam viruses and elevations.

F. Rate limit:

This process provides an extra layer against a mail spoofing by limiting the amount of messages. It uses the sliding window method. In this the limitations can be explained on the basis pf time frames which include minutes, hours and days.

G. BROWSER INTIGRATED TOOLS:

It usually presents on a black list which include URLs of malicious website for determining whether the page related to phishing website or not.

X. THE LINK GUARD ALGORITHM

Link Guard works by analyzing the differences between the visual link and the actual link. It also calculates the similarities of a URI with a known trusted site. The algorithm is illustrated in Algorithm. 1. The following terminologies are used in the algorithm.

v_link: visual link;

a_link: actual_link;

v_dns: visualDNS name;

a_dns: actua lDN Sname;
sender_dns:sender‟sDNS name.

```
int LinkGuard (v_link, a_link}
{
1 _dns=GetDNSName(v_link);
2 a_dns = GetDNSName (a_link);
3 if ((v_dns and a_dns are not
4 empty) and (v_dns != a_dns))
5 return PHISHING;
6 if (a_dns is dotted decimal)
7 return POSSIBLE_PHISHING;
8 if (a_link or v_link is encoded)
9 {
10 v_link2 = decode (v_link);
11 a_link2 = decode (a_link);
12 return LinkGuard(v_link2, a_link2);
13 }
14 /* analyze the domain name for
15 possible phishing */
16 if(v_dns is NULL)
17 return AnalyzeDNS (a_link);
}
```

Algorithm 1: Description of the LinkGuard algorithm.

The LinkGuard algorithm works as follows. In its main routine *LinkGuard*, it first extracts the DNS names from the actual and the visual links (lines 1 and 2). It then compares the actual and visual DNS names, if these names are not the same, then it is phishing of category 1 (lines 3-5). If dotte decimal IP address is directly used in actual dns, it is then a possible phishing attack of category 2 (lines 6 and 7).

```
int AnalyzeDNS (actual link) {
/* Analyze the actual DNS name according
to the blacklist and whitelist*/
18 if (actual_dns in blacklist)
19 return PHISHING;
20 if (actual_dns in whitelist)
21 return NOTPHISHING;
22 return PatternMatching (actual_link);
}
int PatternMatching(actual_link) {
```

```
23 if (sender_dns and actual_dns are different)
24 return POSSIBLE_PHISHING;
25 for (each item prev_dns in seed_set)
26 {
27 bv = Similarity (prev_dns, actual_link);
28 if (bv == true)
29 return POSSIBLE_PHISHING;
30 }
31 return NO_PHISHING;
}
float Similarity (str, actual_link) {
32 if (str is part of actual_link)
33 return true;
34 int maxlen = the maximum string
35 lengths of str and actual_dns;
36 int minchange = the minimum number of
37 changes needed to transform str
38 to actual_dns (or vice versa);
39 if (thresh<(maxlen-minchange)/maxlen<1)
40 return true
41 return false;
}
```

Algorithm 2 The subroutines used in the LinkGuard algorithm.

(Categories 3 and 4), we first decode the links, then recursively call *LinkGuard* to return a result (lines 8-13).

When there is no destination information (DNS name or dotted IP address) in the visual link (category 5), LinkGuard calls *AnalyzeDNS* to analyze the actual dns (lines 16 and 17). LinkGuard therefore handles all the 5 categories of phishing attacks. *AnalyzeDNS* and the related subroutines are depicted in Fig.2. In *AnalyzeDNS*, if the actual dns name is contained in the blacklist, then we are sure that it is a phishing attack

(lines 18 and 19). Similarly, if the actual dns is contained in the whitelist, it is therefore not a phishing attack (lines 20 and 21). If the actual dns is not contained in either whitelist or blacklist, *PatternMatching* is then invoked (line 22).

XI. TIPS TO AVOID PHISHING

i Spell Check.
ii Display name can’t be trusted.
iii Try not to click.
iv Analyze the salutation.
v Don’t share personal information.
vi Beware of threatening language.
vii Review the signature.
viii Don’t make use of all attachments.
ix Don’t trust the header.
x Everything you see is not genuine.

XII. CONCLUSION

Phishing attacks are becoming more relevant attacks from 2010 – 2016 over half of the internet users get at least one phishing email per day. The best defense attacks are to block the malicious emails or messages with the domain based message authentication reporting and conference standards. The vendors must also ensure an intelligence data reveling attacks beyond DMARC unfortunately its obvious that some phishing email will always come into the inbox of various companies automatically and these emails or messages will affect up to 97% of the people who are not able to identify the phishing email. The main process for overcoming this phishing email is to educate the users technically by explaining them about various problems faced nowadays through this phishing attacks. The above explained tips and preventive measures will help the user of the internet to overcome this phishing attacks which results in safeguarding the valuable details money and confidential Data of various users.

ACKNOWLEDGMENT

We take immense pleasure in thanking Mrs. A. Nesarani who guided upon choosing our topic and who taught us the networking aspects of Phishing.

REFERENCES

[1] Yan, Z., Liu, S., Wang, T., Sun, B., Jiang, H., & Yang, H. (2016, July). A Genetic Algorithm Based Model for Chinese Phishing E-commerce Websites Detection. In International Conference on HCI in Business, Government and Organizations (pp. 270-279). Springer International Publishing.

[2] Lininger, R., & Vines, R. D. (2005). Phishing: Cutting the identity theft line. John Wiley & Sons. The Victorian Internet –Tom Standage. Akerlof, G. A., & Shiller, R. J. (2015). Phishing for phools: The economics of manipulation and deception. Princeton University Press

[3] Kadushin, C. (2012). Understanding social networks: Theories, concepts, and findings. OUP USA.

[4] Lininger, R., & Vines, R. D. (2005). Phishing: Cutting the identity theft line. John Wiley & Sons. The Victorian Internet –Tom Standage

AUTHOR'S PROFILE

Mrs A.Nesarani, Assistant professor in Department of Computer Science and Engineering. Her research area includes Internet of Things, Embedded Systems , Network Security and Wireless Sensor Networks.