CHITKARA UNIVERSITY

PHISHING, PASSWORD CRACKING, KEYLOGGERS AND SQL INJECTION, ATTACKS

ON

WIRELESS NETWORKS.

Objectives

- Learn about Phishing and its related techniques.
- Understand different methods of Phishing.
- Learn about Identity Theft and understand ID theft.
- Understand myths and facts about ID theft.
- Understand different types of ID thefts.
- Learn about different techniques of ID theft.
- Get an overview of 3P's of cybercrime (Phishing, Pharming and Phoraging).
- Understand about Spear Phishing.
- Overview of Whaling.

Introduction

- Phishing has become a universal phenomenon and a major threat worldwide that affect not only individuals but also all industries and businesses that have an online presence and do online transactions over the internet.
- The statistics about phishing attacks/scams proves phishing to be a dangerous enemy among all the methods because prime objective this attack is ID theft.

Facts about Phishing

CHITKARA UNIVERSITY

- According to world phishing map available at www.avira.com most phishing attacks are on the rise of Asia, Europe and North America.
- Facebook, HSBC, Paypal and Bank of America are most targeted organization in phishing attacks.
- US, India and China are the most targeted countries.
- Total 3650 non-English (Italian an Chinese) sites are recorded in the month of may 2009.
- The most used TLDs in phishing websites during the month of May 2009 were “.com”, “.net” and “.org” .
- Financial organizations, payment services and auction websites are ranked as most targeted industries.
- Port 80 is found most popular followed by port 443 and 8080.

Phishing

CHITKARA UNIVERSITY

- The word phishing comes from the analogy that internet scammers are using E-Mail lures to fish for passwords and financial data from the sea of Internet users.
- It is criminally fraudulent process of attempting to acquire sensitive information such as username, password and credit card details by hiding as trustworthy entity in an electronic communication.

...cont.

CHITKARA UNIVERSITY

- Phishing is a type of deception designed to steal your identity.
- In phishing technique user tries to get the user disclose valuable personal data- such as credit card numbers, password, account data and other information by convicting the user to provide it under false pretenses.
- E-Mail is the popular medium used in the phishing attacks and such E-Mails are also called Spam's.

Spam E-Mail

CHITKARA UNIVERSITY

- Spam E-Mail are also know as junk mails.
- Botnets, networks of virus infected computers are used to send about 80% of spam. Types of Spam mail are:
  - Unsolicited bulk E-Mail
  - Unsolicited commercial E-Mail

SPAMBOTS

- Spambot is an automated computer program and/or a script developed, mostly into C language to send SPAM mails.
- SPAPMBOTS gather E-Mail ids from the internet, build mailing lists to send unsolicited mails.

CANSPAM

- The CANSPAM act of 2003 was signed in US.
- The CAN-SPAM act is commonly referred to as You can Spam. In particular, it does not require E-Mailers to get permission before they send marketing messages.

Tricks used for Phishing

CHITKARA UNIVERSITY

- Name of legitimate organization: Here phishers may use a legitimate company's name and incorporate the look and feel of its website into the spam E-Mail.
- "From" a real employee: Real name of an official, who actually works for an organization, will actually appear in the from line or the text of the message.

Tricks used for Phishing

CHITKARA UNIVERSITY

- URLs that “look right” : The E-Mail might contain a URL which seems to be legitimate website wherein use can enter the information the phisher would like to steal. However actually the website will be a quickly cobbled – a spoofed website that looks like the real website.

Tricks used for Phishing

CHITKARA UNIVERSITY

- Urgent Message: Creating a fear to trigger a response is very common in phishing attack- the E-Mail warn that failure to respond will result in longer having access the account. Few examples used by phishers to attract the user are:
  - Verify your account
  - You have won the lottery
  - If you don’t respond in 48 hours your account will be closed.

How to prevent from Phishing

CHITKARA UNIVERSITY

- Share Personal E-Mail address with limited persons.
- Never reply a SPAM mail.
- Use alternate E-Mail address to register for any personal or shopping website.
- Don’t forward any mail from unknown recipient.

Methods of Phishing

- Dragnet
- Rod and reel
- Lobsterpot
- Gillnet

Dragnet

CHITKARA UNIVERSITY

- This method involves the use of spammed E-Mail, bearing inaccurate corporate identification (e.g. corporate names, logos and trademark) which are addressed to a large group of people.
- Dragner phishers do not identify specific prospective victims in advance. Instead they rely on false information included in the E-Mail to trigger an immediate response by victims- typically clicking on links on the body of E-Mail to take the victims to the web sites or pop up windows where they are requested to enter bank or credit card details.

Rod and reel

CHITKARA UNIVERSITY

- In this method, phishers identify specific victims in advance, and convey false information to them to prompt their disclosure of personal and financial data.
- For example on a phony web page, availability of similar item for a better price is displayed and upon visiting the webpage, victims were asked to enter personal information.

Lobsterpot

CHITKARA UNIVERSITY

- This method focuses on use of spoofed web site. It consists of creating of bogus/phony website.
- This attack is also known as content injection phishing. The attacker uses a weblink into an E-Mail message to make it look more legitimate and actually take the victim to a phony scam site.

Gillnet

CHITKARA UNIVERSITY

- In this technique phishers introduce malicious code into E-Mails and websites.
- They can for example misuse browser functionality by injecting aggressive content into another site's pop window.
- In some cases, the malicious code will change setting in users system so that users who want to visit legitimate banking websites will be redirected to a look alike phishing site.

Phishing Techniques

CHITKARA UNIVERSITY

- URL manipulation: URLs are the weblinks that direct the users to a specific website.For example instead of www.abcbank.com URL is provided as www.abcbank1.com.
- Filter evasion: This technique use graphics instead of text to prevent from netting such E-Mails by anti phishing filters.

Phishing Techniques

CHITKARA UNIVERSITY

- Website Forgery: In this technique the phisher directs the netizens to the website designed and developed by him, by altering the browser address bar through java script commands
- Flash Phishing: Anti phishing toolbar are installed/enabled to help checking the webpage content for signs of phishing

Phishing Techniques

CHITKARA UNIVERSITY

- Social Phishing: Phishers entice the netizens to reveal sensitive data by other means for example:
  - By sending a mail where ask user to call them back because there was a security breach.
  - The phone number provided in the mail is false number
  - Phishers speak with the victim in the similar fashion as bank employee.

Phishing Techniques

CHITKARA UNIVERSITY

- Phone Phishing: This is known as Mishing, where phisher can use a fake caller ID data to make it appear that the call is received from a trusted organization to entice the user to reveal their personal information.

Objectives

- Understand the security challenges presented by mobile devices and information systems access in the cybercrime world.
- Understand the challenges faced by the mobile workforce and their implications under cybercrime era
- Learn about security issues arising due to use of media players.
- Understand the organizational security implications with electronic gadgets and learn what organizational measures need to be implemented for protecting information systems from threats in mobile computing era.
- Understand smishing and mishing attack in the mobile world.
- Understand security issues due to daily used of removable media.

Attacks on wireless networks

CHITKARA UNIVERSITY

- In this modern world the rising importance of electronic gadgets – which become an integral part of business, providing connectivity with the internet outside the office- brings many challenges to secure these devices from being a victim of cybercrime.
- Today’s Smartphone's combine the best aspects of mobile and wireless technologies and blend them into a useful business tool.

Credit Card Frauds in Mobile and Wireless Computing Era

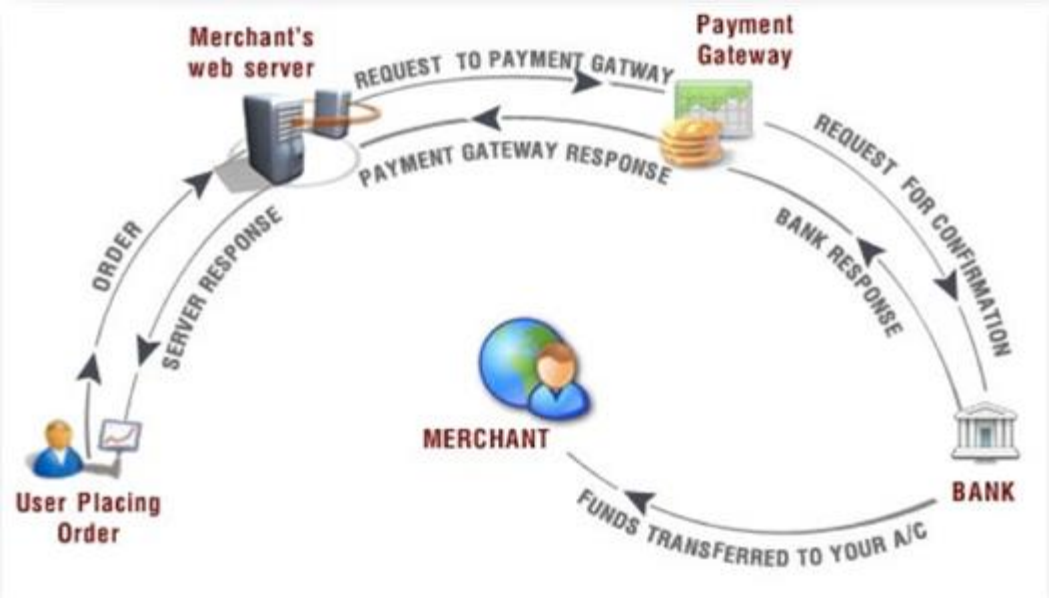
CHITKARA UNIVERSITY

- These are new cybercrime that are coming up with mobile computing- mobile commerce (M-Commerce) and mobile banking (M-banking)
- Today belongs to “mobile computing,” that is anywhere anytime computing. The developments in wireless technology have fuelled this new mode of working for white collar workers.
- Wireless credit card processing is relatively a new service that allow a person to process credit card electronically, virtually anywhere.

Credit Card Frauds in Mobile and Wireless Computing Era

CHITKARA UNIVERSITY

- Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally.



Tips to prevent Credit Card Frauds

CHITKARA UNIVERSITY

Do's

- Put your signature on the card
- Make photocopy of both side of the card and preserve it at a safe place
- Change the default PIN
- Always carry the contact details of your bank.
- Carry your card in a separate pouch/ card holder than wallet.
- Keep an eye on your card while transaction.
- Report immediately if found any discrepancy .
- Inform to your bank if any change in your contact number.
- Report the loss of your card immediately in your bank and at police station.

Tips to prevent Credit Card Frauds

CHITKARA UNIVERSITY

Don’t’s

- Store your card number and PIN in your cell.
- Lend your card to someone.
- Sign a blank reciept
- Write your card number/PIN on any paper/phone.
- Give out immediately your account number on phone

Types and Techniques of Credit Card Frauds

CHITKARA UNIVERSITY

- Traditional Technique
- Modern Techniques

Traditional Technique

- The traditional and first type of credit card fraud is paper based fraud- application fraud, where a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful Personally Identifiable Information (PII) to open an account in someone else's name.

Modern Techniques

- Sophisticated techniques enable criminals to produce fake and doctored cards.
- In this techniques skimming is a technique where the information held on either the magnetic strip on the data stored the smart chip copied from one card to another.

Modern Techniques

CHITKARA UNIVERSITY

- Triangulation: It is another method of credit card fraud and works in the fashion as explained :
  - The criminals offers the goods with heavy discounted rate through a website.
  - The customer registers on this website with his/her, address, shipping address and valid credit card.
  - With the information entered by customer criminal do shopping's from other websites.

Modern Techniques

CHITKARA UNIVERSITY

- Credit Card Generators: It is another modern technique, Computer emulation software's are used to create valid credit cards with valid numbers and expiry date etc.

Security Challenges Posed by Mobile Devices

CHITKARA UNIVERSITY

- There are two types of mobile challenges:
- One at the device level called microchallenges and other at the organization levels called macrochallenges.
- Some well known challenges in mobile computing are: Managing the registry setting and configurations, authentication service security, cryptography security, LDAP, RAS, media player control security.

Registry setting for mobile devices

CHITKARA UNIVERSITY

- Microsoft Active sync acts as a gateway between Windows-Powered PC and mobile-powered devices, enabling the transfer of applications such as outlook information, Microsoft office documents, pictures, music, videos and applications from a user's desktop to his/her device.
- In this context registry settings becomes an important issues, thus establishing trusted groups through appropriate setting becomes crucial.

Registry setting for mobile devices

- According to the experts, the core problem to many of the mobile security issues on a window platform is that the baseline security is not configured properly.
- When you get a computer or a mobile device for the first time, it may not be 100% secure.

Authentication Service Security

CHITKARA UNIVERSITY

- There are two components of security in mobile computing: security of devices and security of network.
- A secure network access involves mutual authentication between devices and the base station or web server, this ensures that only authenticated devices can be connected with the network.
- Thus network also play a crucial role in security of mobile devices

Authentication Service Security

CHITKARA UNIVERSITY

- Some eminent kind of attacks on mobile network due to lack of network security are DoS attack, man-in-middle attack and session jacking attack.
- Security measures in this scenario come from Wireless Application Protocol (WAPs), Wired Equivalent Privacy (WEP), Virtual Private Network (VPN) and Mac filtering.

LDAP Security for Mobile Devices

CHITKARA UNIVERSITY

- LDAP is Lightweight Directory Access Protocol for enabling anyone to locate individuals, organization and other resources such as files and devices.
- In a network a directory tells you where an entity is located in the network.
- LDAP is a light weight version of Directory Access Protocol (DAP), it does not include security feature in its initial version.

LDAP Directory Structure

CHITKARA UNIVERSITY

- Root directory which branches out to
- Countries, which branches out to
- Organizations, which branches out to
- Organizational units, which further branches out to
- Individuals

Media Player Control Security

CHITKARA UNIVERSITY

- Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the music gateway.
- In 2002 Microsoft corporation warned about this, according to them Window Media Player could allow a malicious hacker to hijack people's computer system and perform a variety of actions.

Attacks on Mobile Cell Phone

CHITKARA UNIVERSITY

- Mobile Phone Theft
- Mobile Viruses
- Mishing
- Vishing
- Smishing
- Hacking Bluetooth

Mobile Phone Theft

CHITKARA UNIVERSITY

- Mobile phones are becoming expensive hence increasingly liable to theft. Criminals are interested in accessing wireless service and seek potential possibility to steal the ID
- Keep the following details of your phone
  - Phone number
  - Make and Model
  - Color and appearance
  - PIN and security lock code
  - IMEI (International Mobile Equipment Identity) number

Mishing

- Mishing is a combination of mobile phone and phishing.
- Mishing attacks are attempted using mobile phone technology.
- If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam.
- A typical Mishing attacker uses call termed as Vishing or message known as Smishing. Attackers pretend to be an employee from your bank and claim a need for personal details.

Vishing

- Vishing is the criminal practice of using social engineering over the telephone.
- The term is combination of V- Voice and Phishing.
- The most profitable uses of the information gained through Vishing include:
  - ID theft
  - On line shopping
  - Transferring Money
  - Monitoring bank account details

How Vishing Works

CHITKARA UNIVERSITY

- The attacker often use a war dialer to call phone numbers of people of a specific region.
- When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her account has had unusual activity. The message instruct the victim to call one phone number immediately. The same phone number is often displayed in the spoofed caller ID, under the name of financial company.

How Vishing Works

- When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.
- Once the victim enters these details, the criminal has the necessary information to make fraudulent use of the card to access the account.

Example Vishing

1. Thank you for calling (Local Bank name). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options:
   - Press1 if you need to check your banking details and current balance.
   - Press2 if you wish to transfer funds
   - Press3 to unlock your online profile
   - Press0 for any other query

Cont.

2. Regardless of what user enters the automated system prompts him to authenticate himself: “The security of each customer is important to us, to proceed further we require that you authenticate your ID before proceeding. Please type your bank account number, followed by hash key”.

Cont.

CHITKARA UNIVERSITY

3. The victim enters his/her bank account details and hears the next prompt: “Thank you. Now please type your D.O.B”.
4. The caller enters his/her date of birth and again receives a prompt from the automated system: “Thank you, now please enter your PIN followed by hash."
5. Now customer hears last prompt from system, “Thank you.” Now we will transfer you to appropriate representative.

How to Protect from Vishing attack

CHITKARA UNIVERSITY

- Be suspicious about all unknown callers.
- Do not trust caller ID, it does not guarantee whether the call is really coming from that number, that is from the individual and/or company.
- Be aware and ask questions, in case someone is asking you for personal or financial information, tell them you will call back immediately to verify if the company is legitimate or not.

Cont.

- Report vishing calls to the nearest cyber police cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

Smishing

- Smishing is the criminal offense conducted by using social engineering techniques similar to phishing.
- The name is derived from SMS Phishing

Example Smishing

- We are happy to send our confirmation toward your enrolment for our “xyx club membership” . You will be charged Rs. 50 per day unless you reconfirm your acceptance of your membership on our “Membership office contact xxxxxxxxxx”.
- XYZ bank is confirming that you have purchased LCD TV worth Rs. 85000 only from, website name. Visit www.abcd.com if you did not make this online purchase.

Hacking Bluetooth

- Bluetooth is an open wireless technology used for communication over short distances.
- When Bluetooth is enabled on a devices, it broadcasts its availability.
- The attacker installs special software termed as Bluetooth hacking tools (BlueScanner, BlueSniff, BlueBugger, Bluesnarfer, BlueDiving) for this purpose.

Bluetooth Hacking Tools

CHITKARA UNIVERSITY

- Bluetooth Scanner: The tool enables to search for bluetooth device and extract the information from the discovered device(s).
- Bluesniff: This is GUI based utility for finding bluetooth enabled devices.
- BlueBugger: This tool is used to exploit the vulnerability of the device and access images, phonebook, messages and other personal information from it.

Bluetooth Tools

- Bluesnarfer: Blusnarfer is a tool which extract the data from the phone of a person even his/her bluetooth is off.
- BlueDiving: Bluediving is testing bluetooth penetration. It is similar to bluebug and blueSnarf.

Bluetooth Tools

- Car Whisperer: It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth enabled car stereo.

Physical security

- Cables and hardwired locks
- Laptop Safes
- Motion sensor and alarms
- Warning labels and alarms

Physical Security

CHITKARA UNIVERSITY

- Laptop Safes: Safes made of polycarbonate- the same material that is used in bulletproof windows, can be used to carry and safeguard the laptop.
- Motion sensor and alarms: They can be used to track missing laptops in crowded area, also owing to their loud nature they help in deterring thieves. The owner of the laptop device has a key ring device with a battery that keep the powered on even when the system is shutdown.

Physical Security

CHITKARA UNIVERSITY

- Warning labels and stamps: Warning labels containing tracking information and identification details can fixed onto the laptop to deter aspiring thieves. These labels have an identification number that is stored in a universal database for verification, which in turn makes the resale of stolen laptops a difficult process. Such labels are highly recommended for the laptops issued to top executives.

Security issues due to Removable Media

CHITKARA UNIVERSITY

- With the advancement in technology devices continue to decrease and emerge in new shape and sizes, hence unable to detect and have become a prime challenge for organizational security. Their small size allows for easy concealment anywhere in a bag or on the body.

Security issues due to Removable Media

CHITKARA UNIVERSITY

- Organization has to have a policy in place to block the USB ports while issuing the asset to the employee.
- Disgruntled employees can connect a USB/small digital camera/MP3 player to the USB port of any unattended computer and will be able to download confidential data or upload and malicious software.
- Using Device lock software one can have control over unauthorized access to plug and play devices.

CHITKARA UNIVERSITY

Thanks