SNS COLLEGE OF TECHNOLOGY

(Autonomous)

COIMBATORE – 35

DEPARTMENT OF COMPUTER SIENCE AND ENGINEERING (UG & PG)

Third Year Computer Science and Engineering, 5th Semester

UNIT III - CYBERCRIME: MOBILE AND WIRELESS DEVICES

Topic Name : Attacks on Mobile - Cell Phones

Mobile Phone Theft

Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.

The following factors contribute for outbreaks on mobile devices:

Enough target terminals: The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.

Enough functionality: Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.

Enough connectivity: Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

- Mobile - Viruses
- Concept of Mishing
- Concept of Vishing
- Concept of Smishing

- Hacking – Bluetooth

Mobile Viruses

- A mobile virus is similar to a computer virus that targets mobile phone data or applications /software installed in it.
- Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays. In total, 40 mobile virus families and more than 300 mobile viruses have been identified.
- First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.
- Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS.
- Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth-activated phones (i.e., if Bluetooth is always ENABLED into a mobile phone) whereas MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book.

Following are some tips to protect mobile from mobile malware attacks.

- Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
- If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
- If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
- Download and install antivirus software for mobile devices.

Mishing

- Mishing is a combination of mobile phone and Phishing Mishing attacks are attempted using mobile phone technology.
- M-Commerce is fast becoming a part of everyday life. 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 (SMS) known as Smishing.
- Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.
- Attackers are very creative and they would try to convince you with diff erent reasons why they need this information from you.

Vishing

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V – voice and Phishing.

Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.

The most profitable uses of the information gained through a Vishing attack include

- ID theft;
- Purchasing luxury goods and services;
- Transferring money/funds;
- Monitoring the victims' bank accounts;
- Making applications for loans and credit cards.

How Vishing Works

The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.

1. Internet E-Mail: It is also called Phishing mail.
2. Mobile text messaging.
3. Voicemail: Here, victim is forced to call on the provided phone number, once he/she listens to voicemail.
4. Direct phone call: Following are the steps detailing on how direct phone call works:

- The criminal gathers cell/mobile phone numbers located in a particular region and/or steals cell/ mobile phone numbers after accessing legitimate voice messaging company.
- The criminal often uses a war dialer to call phone numbers of people from aspecific region, and that to from the gathered list of phone numbers.
- 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 bank account has had unusual activity.
- 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 (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.
- Such calls are often used to harvest additional details such as date of birth, credit card expiration date, etc.

How to Protect from Vishing Attacks

Following are some tips to protect oneself from Vishing attacks.

- 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 – caller ID Spoofing is easy.
- Be aware and ask questions, in case someone is asking for your personal or financial information.
- Call them back.
- Report incidents:

Smishing

Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from "SMSPhISHING." SMS – Short Message Service– is the text messages communication component dominantly used into mobile phones. To know how SMS can be abused by using different methods and techniques other than information gathering under cybercrime.

How to Protect from Smishing Attacks

Following are some tips to protect oneself from Smishing attacks:

- Do not answer a text message that you have received asking for your PI.
- Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message.
- Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.
- Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites.

Hacking Bluetooth

- Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances between fixed and/or mobile devices.
- Bluetooth is a short-range wireless communication service/technology that uses the 2.4- GHz frequency range for its transmission/communication.