==========Start lecture 6 notes==========

Q. What is social engineering in the context of computer security?

“The art and science of getting people to comply with your wishes”

Q. Discuss how the formation of inappropriate trust relationships is the basis for social engineering.

Social Engineering involves gaining sensitive information or unauthorised access privileges by building inappropriate trust relationships with insiders.

An outsider’s use of psychological tricks on legitimate associates, in order to obtain information needed to gain access to a facility or system

Getting needed information (for example, a password) from a person rather than breaking into a system

Q. How do social engineers gain a foothold in an organisation’s IT system?

• Social engineers leverage trust, helpfulness, easily attainable information, knowledge of internal processes, impersonation of authority, technology

• Often use several small attacks to reach their final goal.

• Social engineering is all about taking advantage of others to gather information and to infiltrate an organisation.

• Posing as a legitimate end-user

• The irate Vice President

• A published security vulnerability

• Posing as a system administrator

• Calling in looking for someone or specific information

• Use of Search engines to glean information about a company and its associates

Q. Discuss four of the following techniques for social engineering (You should be able to explain all)

Q. Pretexting, Phishing, Spear Phishing, IVR/Phone Phishing, Trojan Horse, Shoulder Surfing, Dumpster Diving, Road Apples, Quid pro quo Q. Describe four social engineering example scenarios

<u>Pretexting</u>

• Pretexting is the act of creating and using an invented scenario (the pretext) to persuade someone to release information or perform an action and is typically done over the telephone.

• It often involves some prior research or set up and the use of pieces of known information (e.g. for impersonation: date of birth, PPS number, last bill amount) to

establish legitimacy in the mind of the target. Often used by private investigators to gain copies of personal records

• This technique is most often used to trick a business into disclosing customer information. • Pretexting can also be used to impersonate co-workers, police, bank, tax authorities or insurance investigators — or any other individual who could have perceived authority or right-to-know in the mind of the company who is being contacted.

• Voice over IP programs are starting to become a standard in pretexting, as it is harder to track an IP address than a phone number, making the pretexter less vulnerable to capture.

Phishing

• Usually involves email but phone calls can be used

• They appear to come from a legitimate business – one you use

• They include a sense of urgency

• There is usually a threat to your personal safety or security

• You are asked to verify personal data

• Banks and other Credit Card Shopping sites are frequent targets

IVR/Phone Phising

• This technique uses a rogue Interactive voice response (IVR) system to recreate a legitimate sounding copy of a bank or other institution's IVR system. • The victim is prompted (typically via a phishing email) to call in to the "bank" via a provided (ideally toll free) number and verify information

Trojan Horse

• Uses your curiosity or greed to deliver “malware”.

• Arrives posing as something free

▪ Attached to email

▪ Screen Saver

▪ An important Anti-Virus or system upgrade

▪ Latest gossip about someone

• Opening attachment loads Trojan onto your computer

▪ Tracks keystrokes, uploads address book, looks for financial software files

Shoulder Surfing

• Prevalent in aircraft, airports, coffee shops, public Wi-Fi areas in hotels, other public places.

• Use of phone/laptop cameras very prevalent

• Observation discloses your logins and passwords.

• Disclosure of credit cards and other High Risk Data.

• Confidential materials can be disclosed.

• Bank ATMs, security locks, alarm keypads.

• Includes “piggy backing” – someone walking into a secure area based on your authentication.

Road Apples • A road apple is a real-world variation of a Trojan Horse that uses physical media and relies on the curiosity of the victim.

▪ CD, floppy, USB Flash Drive

• The attacker leaves a malware infected floppy disc, CD ROM or USB flash drive in a location sure to be found, gives it a legitimate looking and interesting label, and simply waits.

• Once placed into PC to view, the “autorun” feature loads Trojan or virus to track keystrokes

▪ Looks for IDs and passwords

Quid pro quo

• The Something for Something Scam • Two Examples: ▪ Impersonation of a Help Desk ▪ Gift in exchange for Information • Surveys continually show that people are willing to trade private information for relatively low value ▪ Chocolate lure ▪ Cheap pen ▪ Surveys themselves

Q. List five policies that a company or an individual can implement to reduce the risk of social engineering.

• Never share passwords – NEVER, NEVER, NEVER

• Use different passwords for personal and business matters.

• Don’t discuss company confidential matters in public.

• Found CD’s, USB thumb drives? Don’t use them.

• Know how to spot a phish – beware of email attachments.

• Never use a link within an email or call a phone number from within an email – look up the organisation independently.

• Don’t forward or respond to unsolicited email, chain letters and other hoaxes.

• Screen lock your computer when you walk away.

• Don’t share confidential information with strangers over the phone.

Q. Give account of the saying “There is no delete button on the web”.

• While it's exciting to live in an ever connected and always on world, the flip side that we have to accept is that we also live in a world where information is becoming increasingly interlinked.

• Today it is relatively simple to follow footprints on the Web if we want to track both people and brands.

• No delete button on web.

• While the information about me on the Web is not terribly exciting, I do leave a little bit of information on every site I visit.

• Say something in passing on a social site and it may come back to haunt you.

Q. What is a person’s digital footprint and distinguish between active and passive collection of data.

▪ A digital footprint is the collection of all the traces you leave in electronic environments as you use or move through them.

▪ Some is content you actively volunteer—like your Facebook profile.

▪ Other material is passive—the cookies a site stores in your browser, the content your distro collects about your use of their equipment, etc.

▪ All this data can be aggregated to build a profile of you and your behaviour.