Summary Report for Lab Robert Gabriel and Piotr Kawalec.

Introduction

Social engineering was invented and used long time before anyone even thought about social networking or online quiz games. Story of Isaac from The Old Testament or the Trojan horse of the Greeks from the ancient times are just examples of history that accompany humans all the time. It has become more popular with the development of new the technologies. So called ‘effect of Facebook’ gives us an example of how social engineering has grown and is growing area for hacking and gaining personal information about potential victims.

What the report says is that sharing information online can have side effects.

With the Facebook effect, people are adding, and sharing more information online not knowing about the dark side of doing this. The younger generation is sharing more and more online, adding people they don’t know and taking these online quizzes that seem to be friendly (more on this later).

Quizes

People are sharing photos, statutes about family, pets, movies and music they like. All these can tell us a lot about a person and you can build an idea of a person like their favorite color, where they live, who their friends are and much more!

This sensitive data can be a target for any online quiz app.
They (quiz questions) can be obvious (or not) depending from the level of awareness of the targets and the skills of an attacker. User may not realize on time, what is the real purpose behind these questions. In turn attacker has to be cunning enough to hide his actual goal. Presented in introduction quiz ‘**What does your password say about you?**’ is an example of online tool for easy gathering of password information. Study of four presented questions suggests that there is not much work left for trying to guess right combination of characters. It is worth to point out that questions in this quiz (and similar) target specific sensitive data, so if quiz-taker answered them honestly it would indicate to the hacker he is on the right track.

Looking at the overview of a person online, there is one area that it all leads back to. That's the email and with most email accounts there is a password restart feature, where you have to answer a personal question to gain access. This question can be

anything from favorite color, first name of mother and much more. How would a “hacker” gain this information? Well, from the research paper, it's all about getting the information the user gives away on those Facebook quizzes. The user answers, information that seems friendly and safe, but in the background they build a profile of the user, who they are, what's their favorite movie and more. With the use of APIs of Facebook, the Quiz/ app developer (hacker) can ask for permission to the Facebook user’s personal information (email, name, address, friends, location and more).

Most users will not read what permissions the app asks for, so in short by answering short questions about who you are most likely will paint a picture of your character as a person and this can open a can of worms. With this information the hacker can now answer the password restart email question, giving him an access to everything you have online, bank, social media, personal accounts and more into the great theft of gain and identify theft.

Quiz results:

Researches carried out on five Facebook users resulted in profiles made individually for each person. Allowing for quiz to access profile details gathered most basic information: name and email address. Further results compilation shows how seemingly harmless sets of questions-answers allow for developing precisely targeted attack. It can be aimed on quiz victims (phishing email, in person pretexting) as well as third party institutions like banks.

Attack Types

As technology develops different ways of communication, new methods arise for attackers to use them. It also provides environment for safer way of getting the information than if it was physical attempt to obtain information. Today’s social engineering has wide range of tools to use like social networking sites, email services, p2p networks. Often users give a lot of details themselves without knowing who exactly and how will use those information i.e. Facebook account holders give personal details just by assigning to the service. Facebook gives a lot of room for maneuver for information hunters by providing wide access to application developers (quiz and other information gathering authors).

What the report summarises is that as you post information openly online by using the “harmless at first glance” cases it gives cracker and hacker more information about you

to help gain access to your accounts for financial gain. This can be used in the attacks listed below.

The different types of social engineering attempts:

- In-Person Attack or Scam (Face to face attacks)!
- Impersonation & Identity Theft (Pretending to be them)!
- Spear Phishing (sending personal emails, trying to trick them to download software by saying stuff they like and know)

Finish

To finish on this quote from the report.
“Social engineering is like putting together a puzzle. As the social engineer gathers the little bits and pieces of seemingly unimportant information, a much larger picture starts to emerge.**”**