Social Engineering

Venkata SreeKrishna K., Jon W. Meyer, and Adam M. Odell

July 31, 2017
Version 2.1

University of Idaho

CS 539: Applied Security Concepts

Executive Summary

Social Engineering (SE) is a blend of science, psychology and art. Social Engineering in terms of security means the psychological manipulation of people to performing actions or divulging confidential information. While it is amazing and complex, it is also very simple. A social engineering attack can be targeted or opportunistic. Targeted attacks typically focus on a specific individual, whereas opportunistic attacks aim to glean information from anyone in a specific position

Prerequisites

None.

Contents

1 Problem Statement >

- Attackers have shown remarkable success with so called "social engineering" attacks, fooling people into giving them unauthorized access to data, systems and other assets. How do you prevent it from happening?

2 Solutions

1. Develop policies
2. Provide training to employees
3. Measurement and Simulations

1. Employees of an organization must be given a set of guidelines when a particular situation arises.
2. Employees must be given proper training and the different techniques and procedures which are used by the social engineers. They must also be be given the procedure that needs to be followed when an attack has occured.
3. Regularly send out Phishing emails to all of the employees of an organization and see how many click on those.

3 Related News <>

1. RSA SecurID Breach [Dark Reading, 2015]
2. Watering Hole Attack on Bit9 [Dark Reading, 2015]
3. Target Credit Card Theft [Dark Reading, 2015]

1. In 2011 a successful fishing attack utilized a zero-day exploit to install a back door in one of RSA's systems. In doing so, the attackers not only compromised RSA, a high profile computer security firm, but potentially the security of users of RSA's "SecurID" two factor authentication device. [1]

2. A "Watering Hole" attack involves hacking a legitimate website or other net resource to get that site to inject malware into visiting computers. The website is selected because users from the ultimate target are likely to go there. In the Bit9 attack the Chinese hacking group, "Hidden Lynx" gained access to Bit9's digital signing infrastructure and signed malware, making it look legitimate. The malware was then used for further attacks on Bit9 and others. [2]

3. Target stores suffered a breach in 2013 that resulted in 40 million customer credit and debit cards being compromised. It is believed the breach occurred using credentials Target supplied to one of its air conditioning contractors. The credentials were stolen using a phishing attack. [3]

4 Example Scenario <>

"**Mr. Smith:** Hello?
Caller: Hello, Mr. Smith. This is Fred Jones in tech support. Due to some disk space constraints, we're going to be moving some user's home directories to another disk at 8:00 this evening. Your account will be part of this move, and will be unavailable temporarily.
Mr. Smith: Uh, okay. I'll be home by then, anyway.
Caller: Good. Be sure to log off before you leave. I just need to check a couple of things. What was your username again, smith?"
The above Scenario has been taken from the source [9]

Lets look at a sample scenario and then analyze how did he manage to do so.

5 Example Scenario....(Contd) <>

" **Mr. Smith:** Yes. It's smith. None of my files will be lost in the move, will they?

Caller: No sir. But I'll check your account just to make sure. What was the password on that account, so I can get in to check your files?

Mr. Smith: My password is tuesday, in lower case letters.

Caller: Okay, Mr. Smith, thank you for your help. I'll make sure to check you account and verify all the files are there.

Mr. Smith: Thank you. Bye."

The above Scenario has been taken from the source [9]

In this scenario, First the caller tries to convince Mr. Smith that he is one of the Tech support guy from the company and creates a scenario saying that they are going to move accounts. He also convinces Mr. Smith to log off and also confirms whether his user name was smith. Mr. Smith believes in the caller and asks if his files will be lost. So by this move the caller gets a chance to convince him to tell his password in order to check if the files are not being lost.

6 Types of Social Engineering <>

1. Human Based
2. Computer Based

1. Human based social engineering involves the attacker communicating with the target either in person or through a phone conversation. [8]
2. Computer based social engineering involves either automated or targeted communication with targets using computer software. [8]

7 Human based <>

1. Impersonation
2. Important User
3. Third-party Authorization
4. Tech Support
5. In person
6. Dumpster Diving
7. Shoulder Surfing

1. It is very easy to call or approach a company's help desk or reception desk and impersonate someone else in order to gain information. [10]
2. Many social engineers will not just impersonate an employee or patron, but a very important employee, such as a company executive or manager. This puts pressure on their targets to comply with their requests. If the social engineers do not impersonate an important employee, they may threaten to report targets to such an employee if they do not comply with requests. [10]
3. This type of attack can be combined with impersonating an employee. The social engineer will find out the name of someone who has access to assets he wants, will pretend to be a friend or associate of that person, and say that the employee gave him permission to access the resource or information. It's as easy as saying, "Before he went on business trip, Mr. Smith asked me to contact you to get this information". [10]
4. The social engineer will pretend to be the IT guy and say that he needs users to give up certain information or access a certain website in order to solve some crisis. [10]
5. The social engineer enters a corporate employee and impersonates a client or employee. If he is dressed in uniform and sensible security policies are not in effect, he will be able to roam the building. [10]
6. Going through the trash. [10]
7. Looking at the keyboard when someone is typing their password in order to steal credentials. [10]

8 Computer Based <>

1. Popup Windows
2. Mail Attachments
3. Websites

1. A malicious website can create a pop-up window tricking the user into entering his website credentials. [10]
2. Viruses can be disguised and attached to emails. [10]
3. Websites can steal account information through creating a mirror image of a corporate website or email login page and tricking the user into entering account credentials. Alternatively, a website can entice the user to register an account in order to win free stuff and the creator can see if the user uses the same password for all of his accounts. [10]

9 Social Engineering Attack Life cycle <>

1. Research
2. Hook
3. Play
4. Exit

This social engineering life cycle should be seen as a fluid model of attacker behavior. Social engineering attacks are carried out as a single action to capture a single piece of information, as a group of actions to capture multiple pieces of information, or as an impromptu attack that is either carried out without preparation or carried out because of information recently obtained. The research phase is optional, since attackers sometimes carry out attacks in an opportunistic fashion without planning or gathering useful background information that can be exploited. Attackers can repeat this life cycle as often as they wish to keep obtaining more pieces of information to aid a larger hacking attempt. [5]

10 Research Phase <>

1. This phase of the cycle is optional
2. Main Objective is to identify the target.
3. Several sources are used by the researcher:
   - Online Information: Facebook, search engines, social media, indexed public records
   - Public documents: Publicly available government documents and records, leaked voting registers or leaked databases from political parties
   - Physical interaction: Talking to the target or his co-workers, friends, family, or acquaintances

1. Not all attackers carry out this phase, since sometimes social engineering attacks are impromptu. [5]
2. Attackers spend a lot of effort gathering information that can help them identify a target that is easy to exploit, as well as gather information that will help them fool or trick the target. [5]
3. Most of this information gathering can be conducted from any place that has an internet connection. Sometimes it is even preferable to conduct research from another country, since this shields attackers who are caught. [5]

11 Hook Phase <>

- Attacker engages target and provides a pretext.
- There are six influencing levers, which aim to leverage the subconscious
  - Reciprocation
  - Scarcity
  - Consistency
  - Liking
  - Authority
  - Social Validation

- **Reciprocation:** When a target is done a favor or treated nicely, the target feels obligated to comply with the requests of the attacker in order to be courteous. [5]
- **Scarcity:** A target is more likely to comply with the requests of the attacker if they believe that the request must be complied with promptly otherwise the opportunity or the benefit from complying will be lost. E.g., a fake email that warns that an account will be locked unless information is quickly provided. [5]
- **Consistency:** People want to be consistent and keep their word. If a target has promised to do something, he feels compelled to do it so that he doesn't seem unreliable or untrustworthy. This often takes the form of an attacker telling a target false information about a security policy that the target has agreed to for a job and using this to make the target engage in risky behavior that would otherwise be against a security policy. [5]
- **Liking:** If an attacker is well-liked, he is more likely to be obeyed. An attacker who is successful at social engineering is probably likable and charismatic. [5]
- **Authority:** People naturally follow the instructions of authority figures. If an attacker can convince the target that he is an authority figure (e.g., a high ranking executive in the company), then he is likely to be obeyed. [5]
- **Social Validation:** People don't want to be left out of a group or seen as a nonconformist. If an attacker can convince the target that lots of other people are complying with his request, then he is more likely to be obeyed. [5]

12 Play and Exit Phase <>

- The play aims to carry out the purpose of the attack.
- It might be to extract information from the target and keep things going long enough to do so, or it might be to get the target to click on a link.
- The exit phase aims to close the interaction with the target.
- For the attack to be successful, the social engineer will provide assurances so that the victims do not become suspicious and change their passwords.

- In a few cases, the social engineer is not concerned about raising suspicion. This could be due to several reasons:
  - **Lack of traceability:** The intelligent social engineer uses a cheap, disposable cell phone that can be discarded once it has served its purpose and an operation has been completed. [5]
  - **Beyond the reach of law enforcement:** Many social engineers gather information from another country so that law enforcement cannot easily investigate them. [5]
  - **Information received:** If the information that is trying to be obtained is not time sensitive information (such as someone's address or birth date, or intellectual property) then social engineers do not need to be careful of raising suspicion once they have the information. [5]

13 Social Engineering Channels of Attack <>

1. Websites
2. Email
3. Telephone
4. Face to Face
5. Postal Service

1. One of the most common attacks involved setting up a website to direct targets to. The website either delivers malware to the target or acts as a cosmetic copy of another website that the user commonly logs into. The latter is done so that the target is tricked into entering their credentials on the malicious website and giving the attacker access to their account. [5]

2. Phishing involves sending an email where the intention and sender are both disguised. Emails usually trick the target into opening a virus attached to the email or visiting a malicious website. [5]

3. Attackers can use cell phones as a method to easily open up communication with a target. From a cell phone, they can text or call and try to get information directly, or direct the target to visit a link. [5]

4. This channel of attack includes the human-based social engineering attack types discussed previously. It generally involves the attacker approaching the target in person and initiating a conversation in order to gain information. [5]

5. Mail attacks are very uncommon, but they still happen. They usually take the form of the attacker sending the target a letter telling the target that they won some sort of prize (e.g., a lottery) but need to send back specific kinds of personal information in order to claim the prize. [5]

14 Questions I <>

1. Which type of Social Engineering refers to going through trash?
2. How does the attacker engage the target during the hook phase?
3. What is the most common channel of Social Engineering Attack?

Answers are in the appendix.

15 Challenge 1 <>

- For this challenge you will be pairing up into groups of two. Discuss the policies that need to be implemented?

  An example Scenario is present below taken from [7] .

Deliverables: Tell out loud all the policies that you recommend.
Maximum Time available :10 Mins

"One morning a few years back, a group of strangers walked into a large shipping firm and walked out with access to the firm's entire corporate network. How did they do it? By obtaining small amounts of access, bit by bit, from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees' names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they "lost" their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them.

The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. The strangers had studied the CFO's voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system.

In this case, the strangers were network consultants performing a security audit for the CFO without any other employees' knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering."

16 Mitigation <>

- The following can be used to mitigate the risk of social engineering.
  1. People
  2. Process
  3. Technology

The above mitigations will be explained in the upcoming slides of the tutorial.

17 Mitigations: People <>

1. Provide clear boundaries
2. Education
3. Permission to verify
4. Importance of information
5. Create a no-blame culture

1. Employees must be aware of policies and procedures for releasing information and must rigidly follow them. All employees need to know when to refer a request to a supervisor or manager. [5]
2. Employees must be constantly reeducated in training workshops or similar programs to keep them up to date with current security and information handling practices. [5]
3. Employees must feel comfortable in refusing or seeking supervisor approval for requests for information or other kinds of requests. This will prevent employees from feeling intimidated by an attacker. [5]
4. Employees must be taught the importance of all information, even the information that seems harmless, such as phone numbers. [5]
5. Companies must not blame or shame those who are exploited by social engineering attacks. This encourages employees to notify the company of a possible social engineering attack and also prevents attackers from using a successful social engineering attack as blackmail against the person it was perpetrated against. [5]

18 Mitigation: Process <>

1. Bogus call reports
2. Informative block pages
3. Customer notification
4. Escalation route
5. Tiger testing

1. Employees need to report attempted social engineering attacks, especially "bogus calls", or phone calls suspected to be placed by an attacker. [5]
2. Block malicious websites and redirect to a block page that informs employees about the risk of continuing to a malicious website. [5]
3. When the information of a customer is requested and denied through any medium, the customer must be notified. E.g., if someone calls on the phone pretending to be a customer and requesting account information and the information is not given, the company should email the customer and notify them of the failed attack. [5]
4. Front-line employees must have a clear procedure for referring suspected fraudulent messages to a supervisor. [5]
5. Have auditors routinely pose as attackers and confirm that all company security and information handling policies are being followed. Have auditors attempt a social engineering attack in order to confirm that company policies block real social engineering attacks. [5]

19 Mitigations: Techology <>

1. Call recording
2. Bogus lines
3. Email filtering
4. Web filtering
5. Strong authentication

1. While making sure to follow the laws of your jurisdiction, record telephone calls in case an attacker tries to execute a social engineering attack. [5]
2. If a call comes from a phone number range that is suspicious, redirect it to a special line which will apply extra scrutiny. [5]
3. Filter emails suspected of phishing or delivering malware. [5]
4. Block access to malicious websites. [5]
5. Use two-factor or multifactor authentication for logging into accounts or verifying identity. [5]

20 Questions II

1. What type of testing is used to Routinely test staff for their susceptibility to social engineering attacks?
2. Routing calls that are believed to be suspicious is known as?

21 Challenge 2: Policies <>

- Develop five policy recommendations (not including your answer to challenge 1) to help thwart social engineering attacks.

Deliverables: Tell out loud all the policies that you recommend.
Maximum Time available :10 Mins

22 Challenge 3: Training <>

- Develop one creative way to train employees to follow the policies you recommended in challenges 1 and 2.

Deliverables: Tell out loud all the policies that you recommend.
Maximum Time available :10 Mins

23 Conclusion <

- Social Engineering can be a potential threat to an organization.
- An application is always vulnerable to "Human Factor" which is the weakest link in security
- Interaction between a person and a data must be secure than interaction between data and server.

The above information has been adopted from [4]

24 Appendix: Solutions and Change-log <

1. Solutions to the questions
2. Change-log

Questions I

1. Dumpster Diving
2. Pretexting
3. Phishing

Questions II

1. Tiger Testing
2. Bogus Lines

Changelog:

Social Engineering			
Ver.	Date	Authors	Changes
v1	Apr. 6th 2016	Venkata SreeKrishna K. and Jon W. Meyer	First draft of tutorial.
v2	July 19th 2016	Adam Odell	Made major additions, fixed grammar mistakes, and added appendix
v 2.1	July 31st 2017	Ananth Jillepalli	Changed the licensing from CC BY-NC-ND 4.0 to CC BY-NC-SA 4.0

References

[1] Peters, Sara, "The 7 Best Social Engineering Attacks Ever – RSA SecurID Breach", DARKReading. http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?image_number=3

[2] Peters, Sara, "The 7 Best Social Engineering Attacks Ever – Hidden Lynx Watering Hole on Bit9", DARKReading. http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?image_number=4

[3] Peters, Sara, "The 7 Best Social Engineering Attacks Ever – Target Third-Party Take-Down", DARKReading. http://www.darkreading.com/the-7-best-social-engineering-attacks-ever/d/d-id/1319411?image_number=8

[4] Hadnagy, Christopher, "Social engineering: The art of human hacking", John Wiley & Sons, 2010.

[5] Raj Samani, Charles McFarland, " Hacking the Human Operating System", McAfee Labs. http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf

[6] Mann, Mr Ian, "Hacking the human: social engineering techniques and security countermeasures", Gower Publishing, Ltd., 2012.

[7] Granger, Sarah *Social Engineering Fundamentals, Part I: Hacker Tactics* http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

[8] Graves, Kimberly. CEH: Official Certified Ethical Hacker Review Guide: Exam 312-50. John Wiley & Sons, 2007.

[9] InfoSecurity Lab *Weakest Link in the Information Security Awareness Chain?!?* http://www.streetdirectory.com/travel_guide/136960/security/weakest_link_in_the_information_security_awareness_chain.html

[10] Allen, Malcolm. "Social engineering: A means to violate a computer system." SANS Institute, InfoSec Reading Room (2006).