CHAPTER

The Techniques of Manipulation

3

Gavin Watson
Senior Security Engineer, RandomStorm Limited

INFORMATION IN THIS CHAPTER

- Pretexting
- Impersonation
- Baiting
- Pressure and solution
- Leveraging authority
- Reverse social engineering
- Chain of authentication
- Gaining credibility
- From innocuous to sensitive
- Priming and loading
- Social proof
- Framing information
- Emotional states
- Selective attention
- Personality types and models
- Body language

INTRODUCTION

Chapter 2 focused on the social engineering vulnerabilities associated with the business itself. Demonstrating how security weaknesses in the business can translate to the employees. Even the most security conscious employee can become vulnerable due to weaknesses in the business's processes.

This chapter will focus on the most common techniques used by social engineers to exploit human nature, rather than the business. This could be to elicit

Social Engineering Penetration Testing. DOI: http://dx.doi.org/10.1016/B978-0-12-420124-8.00003-X

information or manipulate the target into performing an action that aids an attack. Each of the sections will describe a different technique, explaining why it is used and how it works.

Pretexting

Pretexting is often at the heart of every good social engineering attack, yet has numerous definitions, each adding to the confusion of what it actually is. For example, the Webster's dictionary defines it as:

> *The practice of presenting oneself as someone else in order to obtain private information.*

This is close but is really only describing impersonation. Furthermore, the objective may not necessarily be private information. Various online sources define pretexting in exactly the same way as social engineering is often defined:

> *The art of manipulating individuals into revealing sensitive information.*

It is true that most pretexts are designed to manipulate individuals or elicit information, but this isn't a clear enough definition.

The closest explanation of a pretexting attack was discovered in the Iowa State University's 2009 paper[1]:

> *Pretexting is an attack in which the attacker creates a scenario to try and convince the victim to give up valuable information, such as a password. The most common example of a pretexting attack is when someone calls an employee and pretends to be someone in power, such as the CEO or on the information technology team. The attacker convinces the victim that the scenario is true and collects information that is sought.*

The key part of the above definition is the reference to the creation of a scenario, which is the pretext used to engage the victim. The pretext sets the scene for the attack along with the characters and the plot. It is the foundation on which many other techniques are performed to achieve the overall objectives. A pretext is composed of the following two main elements:

1. **Plausible situation**
   This is the situation that could potentially lead to the objective being achieved. It is a sequence of believable events, designed and guided by the social engineer to extract information or manipulate the target. The chosen pretext is based on the initial reconnaissance. It is this reconnaissance that not only points to a viable pretext but also provides the necessary information to support it.

[1]N.J. Evans, 2009, "Information Technology Social Engineering: An Academic Definition and Study of Social Engineering—Analyzing the Human Firewall," IOWA State University.

2. **Character**
   The plausible situation involves the social engineer playing a "role" much like an actor. This does not necessarily mean impersonating someone real, in fact, it is more often a fictitious character. However, it is important to remember that there are many aspects to consider when creating a character. The social engineer must consider how they would dress, how they would speak and what kind of skill set they would have.

For example, suppose the social engineer would like to elicit bank account information from a member of the public. They have searched through the victim's garbage and found a letter from their Internet service provider (ISP). They decide to use this information to their advantage and build a pretext around it. This attack would likely involve many different aspects but here we just concentrate on the basic pretext that could be used.

For instance, the plausible situation could be:

The victim receives a telephone call from an attacker posing as their ISP. Unfortunately the previous attempt to retrieve the necessary funds via direct debit has failed. If the customer is confident they have the sufficient funds, then the ISP would like to check it isn't a mistake at their end. They would like to confirm the bank account number used, by the victim, and retry the transaction while they are on the phone. If the transaction is successful they will amend their records accordingly.

The character could be:

The caller would be a typical help desk employee, pleasant, polite, helpful and eager to solve problems.

Suppose a social engineer wanted to gain access to a particular business's building. Unfortunately online research had not revealed anything that could be used to aid an attack. However, the social engineer still needs to build a pretext, one that doesn't require any prior knowledge of the business or its processes.

The plausible situation could be:

The business is apparently due a fire extinguisher maintenance check. An attacker, posing as the engineer has turned up to site and needs access to the building to check each fire extinguisher and replace them where necessary. This is not entirely uncommon as these checks are often performed unannounced. The engineer does not need to be escorted.

The character could be:

The engineer would be appropriately dressed in uniform, possibly with various tools. They would only be interested in performing the job quickly and may not react well to delays.

The above two pretexts seem fairly simple but remember that they are only a foundation on which to build the attack. The other techniques described in this chapter can be added to the pretext to make it more likely to succeed. For example, the social engineer may use impersonation, persuasion and credibility gaining techniques to support the pretext to name just a few.

Impersonation

The vast majority of social engineering pretexts will involve an element of impersonation. As previously mentioned, this impersonation need not be of a real individual, instead it will likely be a character specifically designed for the pretext. When designing a character for a pretext the following questions should be asked:

- What would this individual wear?
- How presentable would they be?
- Would they carry any specific type of equipment?
- What kind of accent are the likely to have?
- How well spoken would they be?
- What sort of vocabulary would they use?
- What kind of body language would this person present?
- What skill sets would this person have?

If you cannot answer any of these basic questions then your impersonation may fail. The reason for this is that any inconsistencies in the impersonation will likely draw attention and affect the overall pretext. If someone calls at the door claiming to be a policeman wearing a string vest and sandals, it is unlikely that they will be believed.

Inconsistencies that draw attention can result in validation checks, which will put significant pressure on the robustness of the pretext (not to mention on the social engineer themselves). A validation check could be through asking for details of an onsite contact or to provide valid photo identification. Although such occurrences can be somewhat planned for, such as detailed cover stories and fake badges, they can easily lead to a full exposure of the attack. Therefore, it is critical that you don't impersonate someone with a characteristic that you cannot replicate convincingly.

The aim is to make the impersonation so convincing and so "mundane" as to not attract any unwanted attention. Some social engineers believe that it is not enough to just "play the role", the social engineer has to actually "believe" they are that individual. However, it doesn't really matter how much you believe you are another person, if the victim doesn't believe you due to inconsistencies then your attack will be unlikely to succeed.

If your pretext required the character of an accountant, you may answer the following questions as follows:

- What would this individual wear?
  - A clean and tailored suit, smart shoes.
- How presentable would they be?
  - Very presentable from head to toe.
- Would they carry any specific type of equipment?
  - Brief case, maybe a clipboard.
- What kind of accent are the likely to have?
  - Depends on the region.
- How well spoken would they be?
  - Likely to have formal education, well spoken.
- What sort of vocabulary would they use?
  - Strong vocabulary, especially with financial terms.
- What kind of body language would this person present?
  - Possibly reserved, not overly confident.
- What skill sets would this person have?
  - Strong financial aptitude, bookkeeping.

In social engineering attacks, impersonation is often used to leverage a "real" individual's privileges. When impersonating someone who actually exists, a few challenges present themselves.

The most obvious challenge is learning enough about the individual so as to answer the questions listed above. For example, it is significantly harder to profile an individual to this extent without employing long-term attack strategies, such as long-term surveillance. Clearly if you don't look anything like the individual, then a face-to-face impersonation with someone that knows them is unlikely to succeed. The most common approach is to try and contact the individual, record them and practice imitating their voice. If this can be accomplished then an impersonation over the telephone may well be possible.

There are situations where a real person can be impersonated without having to sound anything like them. For instance, in situations where the victim knows who the person is but has never met them. If you are attacking a large business with many employees, it is unlikely that everyone will have met everyone else. The social engineer could contact the reception impersonating a random new starter, one that the receptionist is unlikely to have met. In this situation the social engineer will probably sound nothing like that individual in any way. In a sense, the impersonation is very poor but it doesn't need to be convincing. Simply by claiming that you are a certain someone, from a certain department, may be enough to gain the credibility you need.

Impersonating individuals via e-mail and written communication would seem like the safest option. However, written correspondence can just as easily contain inconsistencies that may be spotted. When attempting to impersonate an

individual in this way, it is important to gather as many examples of their writing styles as possible. The individual may commonly use certain formalities, informalities, poor grammar or other particular traits. Including such traits like this could increase credibility, whereas not including them could raise suspicions.

When it comes to impersonation the bottom line is "conduct the reconnaissance". If conducted thoroughly, the initial reconnaissance should provide the necessary information to build a robust impersonation.

Baiting

Baiting is a classic technique commonly used by "Grifters" when attempting to swindle money out of their mark. They present an enticing opportunity for the victim and use it to draw them into the scam. In many ways, this can be thought of as a simple bait and trap situation. As long as the target's attention is on the bait, the overall scam may not be revealed.

When social engineers attack businesses to breach the security, swindling money may not be a suitable method. Initially they are more likely to be interested in obtaining information or breaching the computer system. How could baiting be used to breach security?

The initial reconnaissance should reveal enough information to determine whether a particular type of bait is suitable for each viable target. Perhaps your reconnaissance has revealed that the chief executive has a keen interest in classic cars, then your bait could be a rare purchase opportunity.

Once the victim's attention is fixed on the bait, how do you then spring the trap? This obviously depends on what you are trying to achieve. Suppose you want to gain access to a computer system and decide to send a phishing e-mail to someone in the sales department. The most enticing bait for salespersons would be a lucrative lead. The following e-mail is an example of what could be sent:

Hi James,

I don't have time to follow up this lead so do you want it? The client wants to know more about our new services, sounded like a great opportunity.

http://vulnerableinc.com/contact

As long as the e-mail looks right, what salesperson wouldn't click the link, especially if it meant the possibility of commission. If the bait is good enough, the target will often not even think about the legitimacy of the message as the possible rewards are just too good.

One of the most famous and clichéd approaches is by baiting employees with dropped USB flash drives. The idea is that an employee would pick up the drive and attach it to their workstation out of curiosity. The USB drive would contain

malicious software designed to create a backdoor in the computer system. However, there are many variables that cannot necessarily be accounted for, such as:

- What if a nonemployee picks up the drive and attaches it? A back door connection to their computer may breach the "Computer Misuse Act 1990".
- What if the computer does not have outbound internet access?
- What if the antivirus avoidance techniques fail?
- What if the USB ports are disabled?
- What if the employees notice a lot of dropped drives and raise the alarm?

When this attack first originated, all the user would have to do is attach the USB drive, as Microsoft Windows would "auto run" the software within. However, today this is not the case and so other techniques would have to be used. There are devices such as Teensy which will essentially simulate keyboard input when attached, achieving the same back door objective. However, the same challenges discussed above may still apply. One solution is to ensure that only your intended target receives the device. Some professional penetration testers and social engineers have solved the problem by building the Teensy into computer mice, and then sending the mouse as a gift to the target.

Another common physical baiting approach is dropping CDs or DVDs with enticing labels such as Payroll 2014 or staff recruitment plan. However, dropping items such as these inside the premises would be unnecessary as the social engineer is already inside. Instead, items such as these may be passed on to staff via reception or even posted to the target business.

The readers will be most familiar with the baiting techniques used in e-mail phishing scams. The phishing e-mails may contain a promise of money, obtaining free tickets or some other enticing opportunity. This is of course a numbers game and the attacker may only need a handful of victims to achieve their objective.

Pressure and solution

The use of emotional states is a vast subject, especially when related to social engineering. Many of the supporting techniques in this chapter will describe how the social engineer can use different emotional states to their advantage. However, here we will focus on a very specific and effective technique; pressure and solution.

The premise of this technique is extremely simple but the application can be very difficult indeed. The basic premise is to apply pressure to the victim in the form of a negative emotional state such as fear, anger, indignation or shame. Then to present the victim with a solution that would mitigate or remove the emotion. The solution would of course aid the attacker in achieving their own objective. This is similar to baiting as the victim is blinded by the emotion much

like they are blinded by the bait. If you can invoke a strong enough emotion then that is all the victim will focus on.

The following examples show how this technique could be used to achieve social engineering objectives.

- **Fear**
  When we invoke fear in a victim we do not want to reduce them to a quivering wreck, instead the fear could be associated with disciplinary action or losing something important. In theory, the fear could be about anything at all as long as you have a solution that will take it away.

  Objective: Gain access to the chief executives' e-mail account.

  Pressure: The IT department employee receives a call from one of the chief executives who says, "*Listen James, I'm currently sat with two of our clients and I'm trying to walk them through the latest figures. I've typed my password into the mail thing about fifty times and I'm getting nowhere. I thought you guys had things running smoothly over there? I hope you can sort this remotely because it's a long drive over here, which I may make you do.*"

  Solution: This is an awful situation to be in, the very last thing the employee would want to do is start following validation procedures, asking questions that will further annoy the chief executive. In this situation, the employee probably wouldn't think twice before resetting the password. In addition, it would take very little online research to find out the name of a chief executive and their e-mail addresses.
- **Anger/indignation**
  The best method here is to invoke a strong feeling of annoyance, rather than to infuriate the victim. If this emotion is pushed too far you may end up in a situation that quickly escalates out of control.

  Objective: Trick an employee into browsing to a malicious website.

  Pressure: The receptionist is contacted by the IT department, who explain that "*Hi Josie, unfortunately we've detected that the machine you're working on has been used to browse, well shall we say, indecent websites?*". Josie is shocked by the implication "*Well it certainly wasn't me! How dare you*".

  Solution: The IT department could reply with "*Hmm... well there are filters that should block any sites like that, perhaps your machine has been compromised in some way? Could you browse to a few company sites for me so I can check the traffic and find out what's going?*"

Leveraging authority

The previous section included an example of impersonating a chief executive to pressure an IT help desk technician. Although pressure can be applied in a number of ways, as the section showed, that particular example also leveraged the

"authority" that comes with being a chief executive. Taking advantage of authority in all its forms can be very effective for various reasons.

Concerning businesses, one obvious reason is that most employees are expected to perform the tasks set forth by management. The very nature of the employee hierarchal system means that employers can "manipulate" the employees, providing this demand aligns with the expectations of the job role. If the employee believes the social engineer to be part of management, they will likely conform to any reasonable request. Providing management with sensitive information would be unlikely to raise any alarms. In fact, information requests of this kind may well be fairly routine. For example, a social engineer (or private investigator) could contact the HR department of the target business posing as management, requesting information about a specific employee. Provided the HR department believed them to be management they'd likely release the information.

Within a business there are individuals that have authority but don't necessarily fall within the standard employee hierarchy. These individuals act as responsive security controls and also as a deterrent, they are of course security guards. Security guards can be very effective but, in terms of security, they are a double-edged sword. If a social engineer could impersonate one of them, which would likely require little more than a fake uniform, they could use the authority to great effect. The social engineer could ask to see an employee's security badge, maybe even confiscate it. They could claim to be conducting some security checks and want to see the location of keys. In addition, the chances of an employee challenging and questioning a security guard are very slim indeed, even if they didn't recognize them.

> Remember that "authority" needs to be part of every aspect of the impersonation. Looking the part is fairly easy, often a smart suit will suffice. However, sounding the part is more challenging, especially if you don't know what you're talking about. A subtle trick to create the illusion of authority is to ask questions. In a conversation, the person asking the questions is perceived to have the most power. Clearly we're not recommending asking a series of mundane questions and baffling the victim. We're simply saying that the balance of authority could be shifted by something as simple as ensuring that you're asking more questions than the other person.

Here we are focusing on businesses, but authority can also be leveraged in many other situations. The general public are socially conditioned to submit to requests of individuals such as the police, emergency services or even road maintenance workers. If a person dressed in safety clothing tells you to avoid a certain area or use a different entrance, you're likely to comply. Chapter 1 mentioned Operation Camion, whereby terrorists were purchasing emergency vehicles to aid social engineering attacks. If a victim believed the social engineer to be a police officer or ambulance driver, the perceived authority could be leveraged to devastating effect.

> The authors of this book do not in any way endorse or recommend impersonating official bodies such as the police or emergency services. This activity may land you in very serious trouble.

Reverse social engineering

Reverse social engineering is a classic technique used to ensure the attacker has solid credibility. It can involve a great deal of planning and careful timing and can potentially be quite risky. However, if successful it ensures that the victim becomes a metaphorical puppet to be controlled. The basic idea is to get the victim to seek assistance from the social engineer to solve a problem. The social engineer then provides the assistance, which also aids the attack. The victim is requesting something from the social engineer, rather than the other way around. This is why it is called reverse social engineering.

There are various levels of complexity to this technique, depending on the objective. The most basic form involves just one stage: Assist. For example, the social engineer could contact an employee and impersonate someone from the IT department asking "*Are you experiencing any computer issues presently?*" The chances are that someone will have a problem, in fact it is almost guaranteed. The social engineer could then agree to help solve that problem. The challenging part is to work the attack into the solution. For example, the social engineer could claim that they require the user's credentials to log in remotely. Or the social engineer could ask the user to browse to a particular website to test connectivity, which could of course be malicious.

A more complex version of this technique involves two stages: Sabotage and Assist. The social engineer first causes an issue of some kind, then presents themselves as someone who can solve that issue. An extreme example of this would be disrupting utilities, such as cutting off the electric and arriving as a technician sent to fix the outage.

An even more complex version of this attack involves three stages: Introduction, Sabotage and Assist. This technique involves first contacting the victim to gain some level of trust. For example, the social engineer may contact employees and introduce themselves as a new member of the IT department. They could give the employees a direct telephone number, explaining that they can call if they experience a particular computer problem. As the social engineer is not asking for any information or requesting the victim to perform an action it is unlikely to raise any alarms. When such a problem occurs, the victim them contacts the social engineer asking for assistance. The social engineer gains credibility, with the victim contacting them rather than the other way round.

Chain of authentication

The chain of authentication is a powerful technique that can be applied in a multitude of different ways. The concept is to manufacture or orchestrate a situation where the victim "assumes" the social engineer has already been validated. To demonstrate this concept we will jump straight into a simple example.

The social engineer could send an e-mail to a business impersonating a specific customer, requesting information about the service they recently received. The information could be something that only the engineer that performed the service would know. The employee receiving the e-mail could then contact the engineer to retrieve that information and relay it back to the social engineer. The important part of this simple example is how the engineer perceived the situation. From the engineer's perspective, a legitimate employee had requested information that isn't restricted within the company. They have no reason to query the request and they "assume" that the original employee had validated the customer. Therefore, the social engineer gains the credibility of that legitimate employee and indirectly retrieves the information from the engineer. The authentication is passed down the chain gaining strength with each person.

It should be noted that in the above example the "chain of authentication" is a supporting technique to the initial phishing attack. The following example shows how the technique can be used as a basis for an attack, rather than as a supporting element.

Suppose a social engineer wants to gain access to a hospital's server room, perhaps to cause disruption or access patient records. They approach reception posing as an air-conditioning repair engineer. The social engineer explains to one of the receptionists that "*I'm here to perform a maintenance check of the air conditioning units in the server room, the IT department sent me here as apparently you have keys*". The receptionist replies "*Sorry we don't have them, the only person with keys is the porter, his office is just down the hall.*". The social engineers leave and then return a few minutes later saying "*Sorry but no one is answering at the door, I'll try again a little later.*". They could continue pretending to try the door and telling reception that they're not answering, until the receptionist agrees to investigate herself. When the receptionist tries the door, the porter answers and the receptionist explains "*Ah you are in after all, this gentleman is here to do some stuff with the air conditioning in the server room, can you take him up there*". The porter will then very likely assume that the receptionist has already validated the engineer, creating the chain of authentication. This particular example is actually an account of a real attack performed by the authors, demonstrating how effective this technique can be.

Another way of using this technique is to impersonate the employee that makes the validation. For example, the social engineer could impersonate an employee and contact reception explaining that "*. . .an engineer from Vulnerable Inc is arriving in the next 20 minutes or so, can you ensure they sign in and give them a pass to get in and out please. They know what they're doing and where they're going.*". Here the receptionist assumes that the visiting engineer has already been validated by the employee. The social engineer could then arrive posing as the engineer and gain access to the building. In this case, the social engineer forms the start and the end of the chain.

Yet another, somewhat risky, way to use this technique is to present the initial piece of the chain to the victim. For example, the social engineer could contact the

victim saying "*I've just been speaking with your manager Susan, she says that you might be able to help me…* ". The victim may assume that their manager, Susan, has already validated the caller, when in fact they never spoke in the first place.

Gaining credibility

Gaining credibility is a technique used in almost every social engineering attack to increase the chances of success. The idea is to gain credibility with the victim by presenting key pieces of information. This information would be easily obtainable and not necessarily be sensitive, not initially anyway.

If a social engineer was to contact an employee saying:

Hello, could you tell me what version of Web browser you're using?

The employee would likely question why they wanted to know and who they were. The main missing element is a pretext, when added it would result in:

Hello, I'm calling from the IT department, we're performing some remote patching, can you tell if your Web browser has been updated to version 7.0?

Now that we have a pretext the attack is a little bit more convincing, but not much. It can be significantly improved by adding key pieces of information to gain credibility. For example, the social engineer could easily find out the name of the employee they were contacting, the correct name of the IT department, a name of someone who works in IT and maybe a project the business is currently working on. All of this information could be easily and quickly obtained from various online sources.

The attack could then become:

Hi James, it's Simon from the Service Desk, have you got 2 seconds or are you guys still busy with the xyz project? …Ah well listen, we're performing some remote patching, can you tell me if your Web browser has been updated to version 7.0? If not I'll need to send Dave down to sort it out there.

The key pieces of information used in this attack give the social engineer credibility. Even just referring to someone by their name can be enough to make an attack more convincing. Generally speaking, the more difficult to obtain the information is, the more credibility it is likely to give you.

As well as using specific names and referencing business-specific information, using the right business lingo can also be very effective. Perhaps the employees regularly refer to the RSA 2-factor authentication token devices as RSA fobs for example. An attacker could use this to their advantage in a request to the IT department such as "*Hi James, it's Simon from marketing, is Stewart there? Ah well, maybe you can help. I'm just onsite with our xyz client, I need to log in remotely but I forgot my RSA fob again, could I possibly use yours? Can you*

read out what it says?". In this situation the social engineer would have known that Stewart was away, perhaps from an out-of-office e-mail response. Consequently, in this example the names James, Simon, and Stewart all gain credibility, along with the name of the client and the RSA fob lingo.

A great deal of this (credibility gaining) information is discovered during the initial reconnaissance stage, before the attack is even performed. However, the social engineer will likely elicit new information during the attacks that can also be used to gain further credibility. The more sensitive the information, the more credibility will be achieved.

From innocuous to sensitive

The previous section described how to use information to gain credibility. This section discusses another way in which social engineer's use information, or more precisely, how social engineers view information.

From the perspective of a social engineer, "any" information is useful to a certain degree. Previous chapters have described information as being like pieces of a jigsaw puzzle, the more pieces you have the better you understand the big picture. The initial reconnaissance stage performed before an attack could be viewed as collecting as many pieces of the puzzle as possible. However, this analogy can be taken a little further. Each piece of a jigsaw puzzle fits with at least one other piece, which can usually be confirmed with the image printed on the front. Therefore, each piece can be used to identify at least one other piece that fits. To a social engineer any piece of "innocuous" information is a piece of a jigsaw puzzle, one that could be used to identify another, possibly more significant piece of information. The social engineer tries to determine what other information can be obtained using what they currently have. Using innocuous information to identify and obtain sensitive information, then using sensitive information to obtain more sensitive information, is the ongoing process of a social engineering attack.

The example given in the pretexting section regarding a call from the ISP demonstrates this process quite nicely. The attacker first obtained a letter sent from the victim's ISP regarding their current package. This was found in the victim's garbage. This letter does not contain any obvious sensitive information, such as personal details or financial numbers. This is why the victim was happy to throw it away rather than shred it. To a social engineer the letter contains the following pieces of "potential" information, pieces of a jigsaw puzzle that could be used to find more:

- Full name
- Currently used ISP
- Currently used ISP package
- Monthly payment amount
- Account reference number

These key pieces of information can be used to gain credibility and also more sensitive pieces of information from the target. Let's presume that these pieces of information were successfully used to impersonate the ISP and the victim then revealed their bank account number. This is clearly far more sensitive information and allows for more serious attacks to be performed.

Suppose the victim was contacted again sometime later, this time apparently from their bank:

> *Hi is that Susan? Hello there, this is Rachel calling from xyz bank. I'm calling regarding the current account ending in 1234, we believe there may have been a fraudulent purchase made with the associated debit card and we wanted to check the purchase history with you. For security reasons, before we proceed, could you confirm your security password please. Thank you.*

Once the social engineer has the account number and security password they could perform even more serious attacks, maybe even access the bank account directly.

The main point here is to view any piece of information about a target as potentially sensitive, it all depends on how that information is then used.

Priming and loading

The concept of priming (sometimes referred to as loading) is a bizarre and fascinating psychological phenomenon. The basic idea is an individual can be exposed to certain words, ideas or actions that will make them more likely to "choose" associated words, ideas or actions, even without knowing they have.

If the reader is old enough to remember the 1980s children's British television show "Wacaday" with Timmy Mallett, they'll remember the game "Mallett's Mallet." Two children played head to head and each had to think of a word, as quickly as they could, that was associated with the word just said by their opponent. For example, one child may say "*Sun!*", then the other may say "Moon!". If either child was too slow to answer the other with an associated word, they received a foam mallet to the head, courtesy of Timmy himself. In this example, the individuals were trying to think of associated words, which can be difficult when you are put under pressure. However, word association can happen even when we don't intend it to and it isn't necessarily confined to just words.

An experiment that has clearly demonstrated the power of priming was performed by the psychologist John Bargh. Students of the New York University were asked to assemble a four-word sentence from a set of five jumbled up words. For example, the students may have "*ball, running, caught, the, they*" and were expected to produce "*They caught the ball*" or something similar that made sense. One group of students was given sets of words that contained key words

associated with the elderly, such as "*frail, forgetful, grey, balding, etc.*". Once the students had finished this part of the experiment they were told to head to the next stage down the corridor. The researchers timed how long it took each student to walk to the next experiment. They found, as predicted, that the students primed with words associated with the elderly took significantly longer to reach the end of the corridor. Even though the words "old", "slow", or "elderly" were not mentioned, the students made the association without realizing it and it significantly affected their actions.

Manipulating an individual's actions is at the heart of social engineering, so this technique could be very useful indeed. However, the practical application of this in terms of breaching security comes with a few challenges. First, the effect on the individual is not so significant that they'd be willing to do something they know is wrong. Therefore, you couldn't ever "prime" someone into letting you into a restricted area without a really good reason. However, you could potentially prime a victim into a specific state, such as being more "agreeable" for example, that may aid in achieving an objective. The second and most obvious challenge is how the prime is applied without the victim realizing. As we have discussed, the association can happen without the victim knowing, but the application of priming could be very obvious indeed in a real-world scenario. If a social engineer tried to put in key words such as "open", "access", and "granted" into casual conversation then the victim may end up more confused than primed. Priming should be thought of as a supporting technique, and should not form the basis of an attack.

> Priming can also support attacks such as e-mail phishing attacks or attacks via written correspondence. Certain key words could be included that have associations aligned with the objectives of the attack.

In the previous chapter an example was given regarding the issues surrounding customer service mentality. This was a good example of how priming could be applied. By making the victim say "yes" repeatedly it primes them into an agreeable state of mind. The more agreeable they are, the more likely they'll conform to your subsequent requests.

If you decide to use priming to aid an attack consider how much time you have with the target. Also consider what state the victim would have to be in for it to be beneficial and what you would use to make the association.

Social proof

The power of social influence, also known as social proof, is certainly nothing new. Businesses have leveraged social proof techniques for years in order to

encourage people to buy their products and services. The basic idea is extremely simple; people will follow the crowd. It is human nature to seek the comfort that comes with fitting in with everyone else. There are those that actively go against the grain, perhaps in an attempt at rebellious self-expression. However, when the power of social proof is significant enough, they too will likely follow like obedient sheep.

The psychologists Noah Goldstein and Steve Martin are at the forefront of the science of influence and persuasion. One particular experiment they conducted clearly demonstrates the power of influence social proof can have. They investigated the effectiveness of antitheft signage in the Arizona Petrified Forest. The issue was that people were stealing small pieces of petrified wood and thus damaging the natural environment. One of their signs read as follows:

> *Many past visitors have removed the petrified wood from the park, destroying the natural state of the Petrified Forest.*

This had the effect of increasing theft because it creates negative social proof. The park visitors would read the sign and think that "Everyone else is stealing so why shouldn't I?". When the sign was changed to the opposite, stating how the vast majority of visitors didn't steal in order to protect the environment, the theft reduced significantly.

Marketing campaigns regularly fall victim to negative social proof in their advertisements. For example, if they wanted to try and encourage more people to cycle to work, they would have little success using a campaign stating the following:

> *More than 25 million people in the UK don't cycle to work.*

As with the petrified wood sign, this campaign would only make people more comfortable with "not" cycling to work, since so many other people don't do it. The better strategy would be to state how many people do cycle to work and encourage more people to join them.

Social proof is a very powerful marketing tool, but how could a social engineer leverage it? All they need to do is convince the target that other people have complied with the request and then they are far more likely to follow suit. For example, the following excerpt from a phishing e-mail is trying to convince the recipient into clicking the malicious link. However, it is unlikely to receive much response as it falls victim to negative social proof.

> *All,*
>
> *We're trying to push our social media presence. Unfortunately, the vast majority of staff haven't liked our corporate page. Please could you follow the link to remedy this.*
>
> *http://www.somesocialmediawebsite.com/*
>
> *IT Support*

The above request may have some success but if we add positive social proof we're far more likely to receive a response.

All,

Thank you for the great positive response to our social media push. The vast majority of your department have responded with a 'like' and we're really pleased. Join the rest of us if you haven't already using the following link.

http://www.somesocialmediawebsite.com/

IT Support

Social proof can just as easily be incorporated into conversations to aid attacks. For example, a social engineer could simply state that they have already spoken to a number of the victim's colleagues. In this example the names David and Simon act as both credibility and social proof at the same time.

Hey Susan, I have already spoken to David and Simon in your department. They were really helpful and answered most of my questions, send my thanks. However, there were a couple of questions they said you'd be the best person to answer, have you got a couple of minutes to help me out?

Never underestimate the power of people's desire to fit in among the crowd!

Framing information

In the most basic sense, "framing" is about presenting information in such a way as to invoke a specific response or steer the viewer's subjective perception in a certain direction. Normally, framing is used to present information in a more positive way to encourage viewers to "choose" that particular option. For example, suppose you had a choice between two gambling machines that boasted a jackpot of £100. These particular machines were very honest about the odds of winning and advertised it boldly in full display.

The first machine advertised that following:

There is a 35% chance of winning a jackpot with each game played.

And the other machine advertised:

There is only a 65% chance of not winning the jackpot with each game played.

Which one would you choose? Both gambling machines are advertising the exact same chances of winning the jackpot, but you can be sure that more people will choose the first one.

A very common example of framing is how retail stores advertise a sale with statements such as "Up to 50% off!". We all know full well that the vast majority of the items won't be discounted by that much, in fact there may only be a single item reduced by that amount. However, although they could be accused of being

somewhat misleading, they have really just framed the information in a more positive light.

Car dealerships often use framing techniques when it comes to pricing their goods. They will commonly use advertising statements such as "Used cars from £500!" Again, there may only be one car at that low price. Generally speaking, most people will be fully aware that there will likely only be one car at that price. However, the positive framing will still affect their decision, even if only very subtly.

What practical applications are there for framing in social engineering? The previous section contained an example of using social proof but also contained a sentence that took advantage of a "positive" frame.

> *Hay Susan, I have already spoken to David and Simon in your department. They were really helpful and answered most of my questions, send my thanks. However, there were a couple of questions they said you'd be the best person to answer, have you got a couple of minutes to help me out?*

The sentence starting, "... *However, there were* ..." could have easily been phrased like this:

> *... However, they couldn't answer a couple of questions, can you help?*

This puts the same question in a negative frame, which is unlikely to have the affect we want. When phrased in this negative way, Susan is a likely to think "*If they couldn't answer it, why should I be able to?*". By phrasing the question in a more positive way, Susan will be more likely to be agreeable and answer if she can.

As a social engineer, you need to think how your words and actions will be perceived and interpreted. If you can make subtle changes, such as those demonstrated above, you could significantly alter the decisions made by the target. Like with most social engineering techniques, practice makes perfect.

Emotional states

This chapter has already covered the technique of "pressure and solution". That technique invoked a strong negative emotion, then presented a solution to mitigate or resolve that emotion. Pressure and solution is a very effective technique, but it is not the only way in which strong emotions can be leveraged. Arguably, any emotion could potentially aid an attack, depending on what the objective was. Emotions can be used to distract the victim's attention or influence their decisions. The social engineer's challenge is to leverage the emotional state so that it becomes beneficial and not an unstable variable in the scenario.

The first decision to make is whether the emotion will be presented by the social engineer to affect the victim, or whether it will be invoked in the victim themselves. For example, it is far more useful to invoke pity in the victim than show pity yourself. A victim that pities you will be more likely to help in any

way they can, which could easily be leveraged in an attack. Invoking this emotion could take little more than claiming you've forgotten something important, walking with crutches or just playing the fool. However, be careful that your attempts to invoke pity doesn't end up invoking contempt.

Kindness is an obvious emotion to use as the victim is likely to be far more responsive to acts of general kindness. However, this emotion can be used more effectively to take advantage of the power of reciprocation. Therefore, if you can convince the victim that you've done them a favor, they'll most likely want to return the gesture. As social engineering pretexts are often fabricated, the "favor" need not actually be performed, the victim just needs to believe it had been.

Fear is an extremely strong emotion and is one commonly used as part of pressure and solution. However, fear can be used as an effective distraction technique. All that may be required is to set off the fire alarm or call in the bomb scare and the employees will be very distracted. Another example would be for a social engineer to contact an employee at their home explaining that someone has broken into the office. They explain that there is broken glass everywhere and a lot of equipment and personal items appear to have been stolen. The victim can hear the office alarm clearly in the background. The social engineer then explains "*The police are on their way so I'll keep you posted, there's no need for you to come down. I've tried to disable the alarm but it's not working, what code do you normally use*?". The fear keeps the victim distracted and less likely to question anything about the situation.

Trust is another emotion that can be easily leveraged. Many readers would argue that trust is not an emotion but rather a perception of another person. However, it is possible to invoke trust in a person, just as you would invoke any emotion. A female social engineer displaying a pregnancy bump would certainly invoke a great deal of trust in those around her. Should the fake pregnancy bump contain tools such as lock-picks and drop boxes then you'd have a very dangerous social engineer indeed.

Any emotion can be leveraged by a social engineer, they are limited only by their imagination. However, it should be noted that emotions are, by their very nature, unpredictable at best. A carefully planned exploitation of a strong emotion could easily turn into a tirade of uncontrollable events, resulting in a very difficult situation for the social engineer to manage.

Selective attention

Selective attention is a fascinating phenomenon regarding how we process information. It is sometimes referred to as the "cocktail party effect". The reader may have experienced this effect when in a crowded room, when they are able to single out and understand a single voice among the many others. We are able to almost filter out the unwanted sounds in the sense that we don't process them,

although we can still technically hear the noise. The only sound we process is the one we want to. In this example, the individual is purposefully filtering out the information. However, this effect can happen in many situations whether the individuals want it to happen or not. The simple reason for this is that our various senses receive far more information than we could ever hope to fully process. Therefore, the vast majority is buffered and our minds filter this information so that only the most important pieces get through. Attempts have been made to fully understand the details of this process such as the Broadbent, Treisman, Deutsch & Deutsch and Kahneman models for selective attention. A full discussion of these models is far beyond the scope of this book. However, the possibility of exploiting this phenomenon to aid in social engineer is within scope.

Unintended selective attention is famously demonstrated in the 1999 video by Simons and Chabris. The video shows individuals, some dressed in black, others in white, passing basket balls to each other. The viewer is asked to count how many times the individuals dressed in white pass the basket ball. Approximately half way through the video a person in a gorilla costume walks to the center of the activity, waves at the camera and walks off the screen. At the end of the video the viewer is asked how many passes they counted. The vast majority of viewers do not notice the gorilla. I myself did not see it when watching this video for the first time and even had to watch it again from the beginning just to prove it was indeed there. The viewer's attention is so transfixed on the complicated passing that they do not process the clearly obvious event of a gorilla waving right at them.

This video proves that it is possible to manufacture a situation or sequence of events that prevents the victim from processing certain information. Preventing victims from seeing the waving gorilla is obviously not that beneficial to a social engineer, however, the basic premise could be replicated to aid in an attack. All that social engineer needs to do is ensure the victim's attention is focused on something complicated enough to prevent any other information from being processed. The "anything else" would of course be the element that achieves the objective.

How does this differ from basic distraction techniques? In many ways, leveraging selective attention could be thought of as advanced distraction. Rather than being the clichéd:

Hey, what's that over there?

Instead the social engineer could ensure the victim's attention is fully focused on a specific task. Though a real-world application of this may well take a great deal of creativity.

Personality types and models

Personality typing has been around since ancient times and there have been many different models over the centuries. The various theories surrounding personality

typing could fill many volumes. The idea of placing individuals into specific groups and then using those groups to predict their behavior has the potential for incredible applications. If you can accurately and consistently predict your own actions based on your own personality type, then you can use that knowledge to maximize your strengths and reduce your weaknesses. You could determine which people would be best assigned to certain tasks, build teams that cooperate effectively and gain great insight into disputes.

From a social engineering perspective, you could adjust your approach based on the target's personality type to maximize the chances of affecting their decisions. This all sounds fantastic but unfortunately, as with many areas concerning human nature, personality typing is far from an exact science. You can certainly place individuals into personality type groups and even predict their actions with a pretty good degree of accuracy, but it is far from having a guaranteed outcome. The problem is that personality can change over time and no one really knows how personality is affected by influences such as genetics, upbringing, personal experiences and culture.

Trying to influence individuals based on personality type comes with significant challenges. Personalities shift and change by the moment based on circumstance and individuals may have a personality that spans multiple "distinct" groups depending on the model used to interpret it. The authors believe that influencing by personality type is not entirely practical in "short game" based real-world social engineering assessments. We fully expect many professional social engineers to react strongly to this statement claiming that they've consistently had great success. However, the authors stand by the belief that it should never form the basis for an attack, unless you have enough reconnaissance time and/or interaction with a target to be confident that a certain personality type-based approach would be effective.

Reporting to a client that a specific security guard falls within the "analytical" personality group and therefore responded more significantly to "authority" is not particularly valuable to a client. There are likely more pressing vulnerabilities concerning procedures, policies and awareness training that need to be identified and reported on first. However, that being said, there would be value in conducting awareness training based on how a social engineer may "attempt" to leverage certain personality types. Training workshops on the strengths and weaknesses of certain personality types could be quite beneficial to employees. The point here is not to make personality type issues a priority or even a focus until the more concrete security problems have been remediated.

As previously mentioned, there are many different personality type models and much has already been written on how to influence each specific type. However, in an attempt to keep the content of this book as "practical" as possible, we will only discuss the supporting technique that we as professional security consultants have regularly used during assessments. As a supporting technique, influencing based on personality types can increase the chances of success of certain social engineering scenarios. Generally speaking, a proof of concept is all that is required in each

scenario, so one success is sufficient. Nevertheless, occasionally a greater degree of success can add a "worst-case scenario" element, which the client may find useful (as leverage to release security budget for example).

The personality type model we regularly use is Jung's theory of the "introvert" and the "extrovert." This theory places everyone into two distinct categories with opposing behaviors. The introvert finds their internal reality to be more real and are generally motivated by subjective matters. Individuals within this category are described as being introverted, which is synonymous with being quiet, thoughtful and reserved. The extrovert finds external reality to be more real; they usually define their existence based on their relationship with other people. Extroverts are often described as being extroverted, which usually means confident, chatty and outgoing.

The reason we use this model in social engineering engagements is for two main reasons. First, it is relatively easy to determine which group an individual belongs to. Introverts tend to be quiet, shy and inward thinking, while extroverts are the complete opposite, and although this is certainly not always the case, it is consistent enough to have a practical application. Second, influencing each group is straightforward, based solely on the absolute basics of the theory. For example, as extroverts define their existence based on their relationships with others, then logically they will be more susceptible to techniques such as social proof. As introverts tend to be more subjective, placing ideas in terms of how it affects them personally would be more effective.

Additionally there is the aspect that introverts tend to be friends with introverts, extroverts with extroverts. Consequently, in terms of establishing good rapport with someone who is clearly an introvert, storming in with a big personality may not be entirely effective. Good rapport can have a significant effect on decisions made by the target, so mirroring their group can be very effective indeed.

Relationships tend to be made up of one introvert and one extrovert. Some theories state that this is because we look for a partner that would compliment our personality, opposites attract for example. Based on this, an outgoing and friendly female may be more effective at influencing an introvert male and vice versa.

As previously mentioned, we would never base an attack on these theories. However, we do consider their possible implications on a scenario and whether they may hinder or aid the attack.

Body language

Only a tiny proportion of communication between two people is based on spoken words. A much larger proportion is based on the pitch, speed and tone of the words. An even larger proportion still is based upon body language. To demonstrate this, imagine you have been summoned to your boss's office for a dressing down. Your boss is stood with his hands on his hips towering over you, his face

shows a look of general disdain. Their voice is booming as they describe how you've failed to meet their expectations in a recent project. Everything about this situation is unpleasant and communication is very clear; you've messed up in a big way. Now, suppose your boss is saying the exact same words, in the same booming voice, but this time is cowering in the corner of the room, sat with hands around his knees. This would be very odd indeed and you would likely not know what to make of it. Chances are you wouldn't feel half as threatened and the words would lose all meaning. The body language takes precedence over the voice and words. Similarly, if your boss was to describe your failure to meet expectations in a squeaky mouse like voice, they probably wouldn't have much impact at all.

Body language is a hugely influential part of social interaction. For example, in the military where people have earned "positions of power" but are physically short in stature, they may use creative ways of overcoming these barriers. Such as the 5 ft 2 Regimental Sergeant Major (RSM), who has the most feared rank in the British Army, may place his desk on a raised plinth so that when subordinates are called in for disciplinary matters they will always be in a lower, subservient, position.

The power of body language to influence others is significant and can help to support social engineering attacks. There are two ways in which body language techniques can be applied. The first way is to adjust your own body language to affect the target. An example of this would be using confident and dominating body language to support the impersonation of a chief executive. The other way is to "read" the body language of the target and adjust your approach accordingly. For example, if the target's body language is suddenly very closed off then you may want to consider an alternative approach to your inquiries.

Mirroring another person's body language is a common technique to improve rapport. Be careful though, as mirroring too obviously could end up disturbing the other person, especially if they realize what you're doing.

Adjusting your own body language as a supporting technique is very straightforward to apply and can have great results. There are many different aspects of your own body language that could affect the target, here we will cover the most common.

- **Smiling**
  This seems like an obvious type of body language, surely the target will respond better to someone that is smiling. While this is generally true it is important to understand the difference between a real and a fake smile. A real smile can be seen in the eyes as the cheeks, sides of the eyes and eyebrows all raise up. A real smile is difficult to fake as the muscle movement involved tends to be subconscious. However, it is possible to fool a target into believing the smile is real and this can be extremely beneficial. If the target subconsciously picks up on an apparently genuine smile they will respond far more agreeably. Never underestimate the power of a good smile.

- **Posture and presence**
  If you need to come across as confident as part of the impersonation, then your posture and presence can have a huge impact. If you are sitting up straight as opposed to slouching, then you present confidence to those around you. Similarly, sitting back with your arms spread out to dominate the space you occupy also presents confidence and power.
- **Eye contact**
  Eye contact is a huge area of communication and if you don't consider it during an impersonation it could give the game away. Not making eye contact or continually looking away is often considered a sign of weakness or shyness. If you are struggling with an impersonation or having doubts about the success of a scenario midway through it, your eyes may give you away. On the other hand, making eye contact for too long could be considered aggressive or disturbing.
- **Arms and legs**
  The idea of arms and legs being read as being open or closed is a common one regarding body language. There are those that claim that even the position of someone's feet can give away their inner feelings. A more practical approach is to consider more than one element regarding an individual's position concerning their arms and legs. For example, if someone has their arms and legs crossed and they're sitting sideways on to you, then you can be pretty sure they're not exactly engaged with you or what you're saying. Whereas is they're leaning across toward you with arms open they're probably quite interested. Consequently, if the target is closed off then your approach is probably not working.

A fascinating area of body language known as "Micro Expressions" was pioneered by Paul Ekman in the 1990s. A microexpression is an extremely brief (1/25 to 1/15 of a second) involuntary facial expression that reflects the persons emotions. This commonly occurs when the person is trying to conceal a particular emotion. Leveraging this research would mean that you could potentially know what a person is truly feeling and maybe even detect if they're lying.

SUMMARY

This chapter has covered a great deal of ground, introducing the reader to many different social engineering techniques. The variety of techniques discussed is testament to the broad reach of exploiting vulnerabilities in human nature. The reader has been introduced to techniques that exploit emotional states, employee hierarchy, trust relationships and a variety of psychological tricks to name just a few.

These are the primary techniques on which many social engineering attacks are based and we have only just begun to scratch the surface on what is possible.

However, understanding these techniques and concepts is not enough to perform effective attacks, especially in terms of a social engineering assessment. The application of these techniques is also just one part of the overall social engineering assessment process. These are just the tools in the social engineer's kit. The true skill of social engineering is knowing which technique to use and when.

The next chapter will discuss the difference between short-term and long-term attack strategies, when each should be used and what their individual strengths and weaknesses are.