Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung
http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

Social Engineering - The Most Underestimated APT

Hacking the Human Operating System

Dominique C. Brack

Social Engineering is an accepted APT and is going to stay. Most of the high-value hacking attacks feature components of social engineering. Understanding of the methods and approaches used behind the scene of Social Engineering will help you to make the world a safer place. Or make your attack plans more successful. This article is based on a book I recently wrote about Social Engineering. As a bonus I will present the readers with a free download code for ebook-versions (PDF, epub, mobi) of my book for further study.

Citation: Brack, D. C. (2017). Social Engineering - The Most Underestimated APT: Hacking the Human Operating System. (Volume 14, Pages 830–857). Retrieved September 18, 2017, from http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_056_Brack_SEET.pdf

Version 2017/11/08 18:16

1 Social Engineering

As a senior security professional I work with many clients.
International, local, governmental, defence clients in highly sensitive settings (politically or regulatory). For them, I am always going the extra mile or two. Some of my clients experienced highly sophisticated spear phishing attacks and attempts of industrial espionage. To address these types of attacks I started to collect best practices and I've developed additional methods for dealing with Social Engineering in its many facets. Soon I realized that the problem of Social Engineering is systemic and grossly underrated even by security professionals. Social Engineering has progressed and professionalized more than you think. It is disastrously effective. In order to adress this issue, to raise awareness and to be able to communicate my findings to all of my clients and other people at the same time I decided to take action. Together with my business partner in Germany, I wrote a book. «Social Engineering Engagement Framework (SEEF) – FIRST CUT« is available as paperback and ebook. As supporter of the DeepSec conference you, dear reader, will be given a download code for a free download of the complete ebook and its Social Engineering icons. You find the download code in the Appendix of this article, at the end of this chapter.

The following article is an excerpt of our book, a summary of its most important parts.

When it comes to Social Engineering the media often refers to people as «the weakest link,«. On the contrary, I actually believe that people are the strongest and best link you will ever have to fight Social Engineering. People are flexible when it comes to decision making and they are able to execute tasks based on intuition. Many amazing tasks were only achieved because people are not machines but human beings, who sometimes make irrational decisions. No machine would rescue a cat from a tree or selflessly try to save someone's life. We need people to stay people and machines to stay machines.

2 Social Engineering Engagement Framework (SEEF)

SEEF has been invented and developed by Dominique C. Brack, aka »D#fu5e,« and Alexander Bahram, aka »4en5icr.« The framework is based on our personal work experience coming from decades of practical application of information-security principles on an international level.

As professionals in the information-security field, we understand the challenges and know what it takes to protect and safeguard corporate assets, because we have helped many of the world's most dynamic and ambitious companies to develop their information-security posture. We aim to lead the Social Engineering profession by delivering visionary leadership projects like the Social Engineering Engagement Framework (SEEF), setting the benchmark, aiming for the highest ethical and professional standards. Our goal is to improve Social Engineering as a discipline and add transparency and professionalism to it, to produce comparable and reproducible results and reduce risk in the process.

There are many different definitions of Social Engineering, but none of them seemed to fit our purpose. Therefore, we had to create our own definition of Social Engineering as we understand it. We feel this definition matches up perfectly with what we understand as Social Engineering. SEEF defines Social Engineering as follows:

»The elicitation of information from systems, networks or human beings through methods and tools«

In today's highly complex business structures, more advanced methods for Social Engineering are necessary. Social Engineering is a fairly new discipline that is sometimes complex, relatively unstructured and not yet fully developed.

But it already has become an engineering discipline with precise tools, selected dynamic approaches and execution plans. This makes it so damn hard to define countermeasures against SE attacks on the receiving end. You never really know where you could get hit next. But as with all things, the best strategy of detection and defense (active/passive) is to stick to your own processes, raise awareness and train your staff, employees and especially your senior executives.

SEEF focuses on the **human part of Social Engineering**, **not on the underlying technology** supporting Social Engineering.

SEEF addresses different stakeholders. Not all the topics in the framework will appeal to everyone. This is the reason why we defined three stakeholder groups. Every group has its specific field of interest in the framework. Whether you want to become a Social Engineering expert or just get yourself up to date concerning the latest developments and associated risks of Social Engineering, you will find specific content tailored to your needs.

The framework defines three groups of key stakeholders.

- Professionals (Ps)
- Organizations (Os)
- Governments (Gs)

Professionals comprise the group of individuals who have a professional interest in Social Engineering, people in functions or roles requiring Social Engineering knowledge either for active use or for building protection against Social Engineering attacks. Some examples might include the following:

- Chief Information Security Officer (CISO)
- Risk Managers
- Project Managers
- Risk & Compliance Officer

- Privacy Officer
- Consultants
- Freelancer
- Hackers

Organizations comprise the stakeholder group whose companies and other professional bodies take a vested interest in Social Engineering. This could be any of the following:

- Private intelligence companies
- Big 4 consulting firms
- SE companies
- International organizations
- Information-security companies

Governments include public-sector interests. These are the people who can devise, pass and enforce laws and regulations. The groups included in this stakeholder group could be the following:

- Intelligence organizations
- Military
- Universities
- Diplomatic relations
- Strategic security
- Nation-states
- Policymakers

2.1 Engagement Management

The Social Engineering engagement management method is comprised of three individual core processes. The core processes are as follows:

- Pre-engagement process group
- During-engagement process group
- Post-engagement process group

The pre-engagement process group contains all the processes that are relevant and required before you start and begin the engagement. The Pre-engagement process group is about prepping your engagement. Included are specific social-engineering processes for controlling, mitigating and managing risk. No other engagements, like IT projects or others, require these specific processes. It is about setting the scene and making sure you have covered all necessary basic requirements for starting a social-engineering engagement.

After every single step from the pre-engagement process group has been executed, the actual engagement begins. **This is the »hot« phase of your engagement.** This process group is called the during-engagement process group. The social engineers are at work and need to be monitored for support or extracted in case of trouble. There is constant monitoring of risk, status and progress.

Post-engagement process is labeled PosE. This phase delivers the results to the client and formally closes the project.

Social Engineering has some specific requirements in terms of risk management and execution. The SEEF engagement management offers you a detailed view on those processes . The defined processes fit a large, international and risk intense project. For smaller projects, you tailor the processes accordingly or you adopt the SEEF engagement management processes into your risk/ project management framework. The minimum recommended processes for SE projects are:

- ***1.1 Client Selection & Acquisition***
- ***1.1.1 Client & Job Risk Assessment (Scope, Method, Approach)***
- ***1.2 Scoping & Approach Selection (Methods, Tools and Skills)***
- ***2.1.1 Deliverables & Approach Monitoring***

Process 1.1 Client Selection & Acquisition

The first step in the pre-engagement process group is client selection and acquisition. Before you even send out a proposal or reply to an e-mail request, this step must have been executed. For the evaluation, if a client or a project is acceptable, you can use the following criteria:

- Use the GRC++ criteria (i.e., intensity levels, ethics and culture)
- Credit rating of your client's company
- Ownership of your client's company
- Type of company to engage with (government, non-government, not for profit, politically active, ethically questionable, black hat, hacktivists, etc.)
- Reputation of the company
- Geographical and cultural fit
- Skills and capabilities match
- Workload and resources consideration

If you are asked to execute an engagement, tasks or to engage in activities above your threshold intensity level, then you have to refuse the tasks, project or engagement. The same applies if the request is misaligned with your cultural and ethical principles or any other criteria you set for yourself or your company.

For Social Engineering, penetration testing and information-security work, your biggest asset is your reputation. Keep your reputation well-guarded and constantly work on it.

Process 1.1.1 Client & Job Risk Assessment (Scope, Method, Approach)

Immediately after you have accepted the client, project or task, you have to set up the ongoing monitoring process for the client and job risk assessment as well as monitor the scope, selected methods and approach you have selected. There are two general areas you have to monitor constantly until the engagement, project or task is finished:

- The client
- The project (i.e., the scope, selected methods and approach you have chosen)

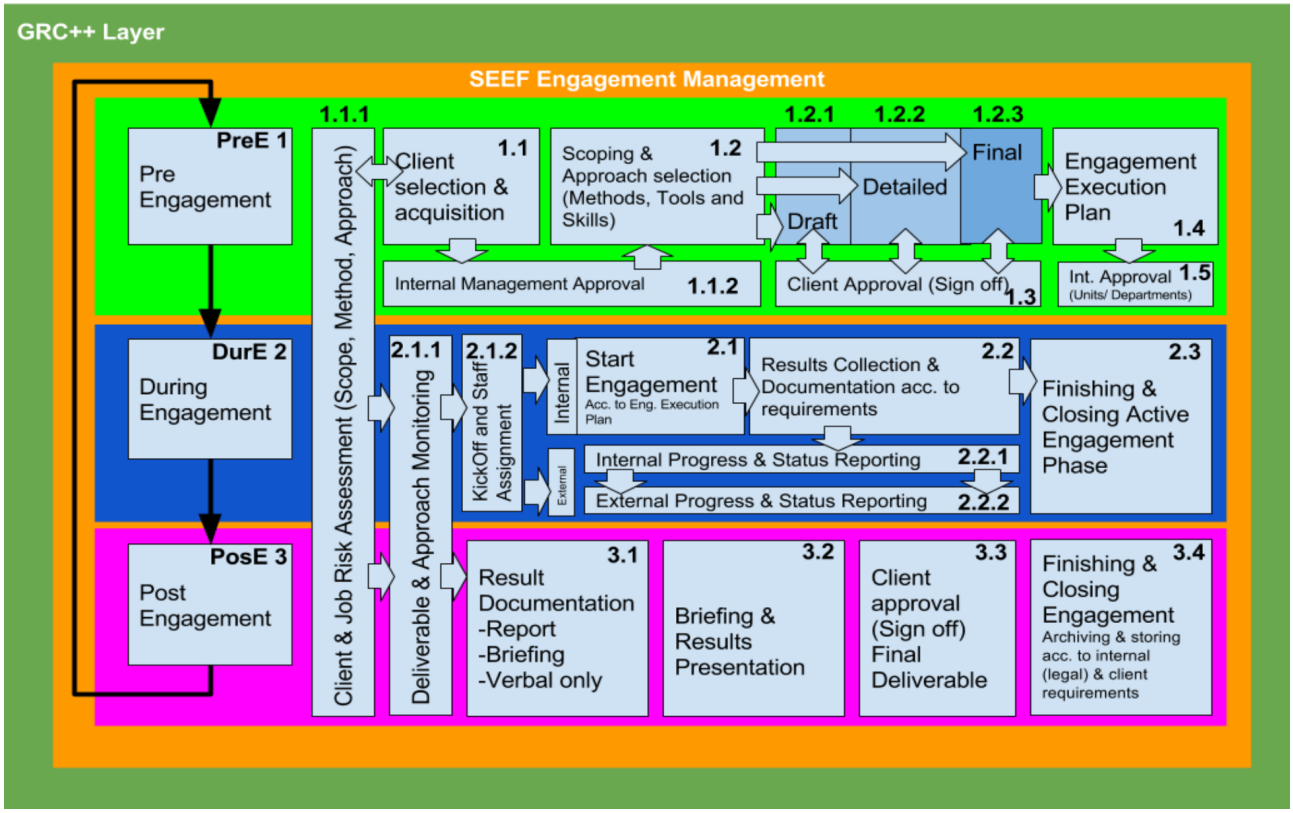


Figure 1: Engagement Management Overview

These parameters can change at any time during your project, engagement or task execution. For instance, your client may be involved in a huge, never-before-seen scandal. In that case, you should register this and make an informed decision about whether your basic principles of GRC++ or any other of your cultural, ethical or work principles are still compatible with working for this particular client and whether you want to proceed with your work or not. In extreme cases, you might have to cancel the project, engagement or task according to observations you make about your client. Many things can go wrong; for example, the client might go bankrupt or get involved in illegal activities, a legal case might collide with your Social Engineering, a client might be subpoenaed, the client's location might be quarantined, a war might start, etc. Usually, you do not have to deal with these types of exceptions, but you must be prepared and have the process in place to react professionally and swiftly. During the project, the scope might get extended or adjusted or you may experience scope screep, which means you must reassess whether you're still within your boundaries. The client & job risk assessment process is very important and often gets forgotten or is only partially done. It is important that someone who is reliable and experienced monitors this process.

Process 1.2 Scoping & Approach Selection (Methods, Tools and Skills)

Finally, after all these time-consuming activities, scoping and approach selection begins. Based on the requirements, you start laying out the scope of the project and choose your approach accordingly. For more simple projects, you might use well-known attack vectors and successful approaches you used in the past. The two SEEF methods help you with this activity: attack-vector development and approach-selection method. Use those two methods to describe your scope and approach. The client will have to sign off on the scope, the selected approach and the planned attack vectors including the risk associated with these tasks. Depending on the size and scope of the project, you can create a draft or a detailed or final document. The goal of this activity is creating full transparency for you and your client on the risks, costs and impact of the planned activities.

Process 2.1.1 Deliverables & Approach Monitoring

This process establishes the monitoring of the defined deliverables and the selected approach. It is very important to constantly check whether the project is delivering the expected results and is also able to achieve them. If this is not the case, then corrective action has to be taken.

2.2 Governance, Risk and Compliance including »++«

For our Social Engineering engagement framework (SEEF) we felt it would not be enough to consider only governance, risk and compliance (GRC) for our engagements. A SEEF exists not only to protect the individual who is working on Social Engineering en-

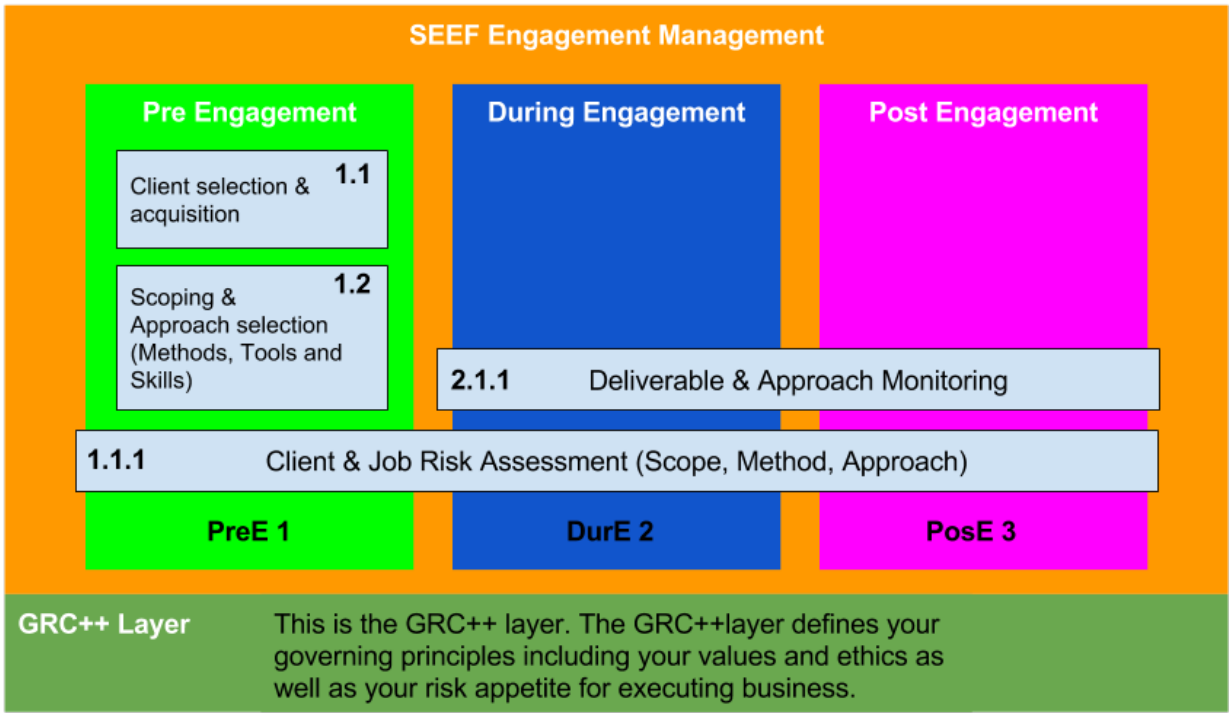


Figure 2: Four most important process for Engagement Management

gagements but also to protect the company that is engaging in such activities. Before SEEF, Social Engineering engagements carried too much risk and uncertainty. From our own experience working for the Big 4 in highly complex and politically delicate international settings, we know firsthand how hard it is to manage risk appropriately.

For this reason we have developed the GRC++ approach for Social Engineering and why we added the »++« to the GRC standard.

2.3 The GRC Standard

Governance: Governance is a senior-management-level activity. It clarifies who holds the authority to make decisions and is used to determine accountability. Sound governance structures can be established by creating groups such as steering committees to bring the right parties together to make decisions. Lack of governance can result in irrational goal setting and decision making. This eventually ends in turf battles, wasted resources and conflicts. For a Social Engineering engagement, the following questions should be asked: Have I applied the right methods and tools? Have I managed risk appropriately? Am I in compliance with laws and regulations?

Risk: Risk represents the possible adverse impacts of reaching goals, and it can arise from actions taken or not taken. A carefully implemented risk management process helps to set priorities and determines the level of effort that goes into reducing the likelihood and magnitude of risk. Good risk management identifies risks and provides open discussion about the best approaches for handling risk. A culture of risk management helps to prevent ignorance and thus reduces negative consequences.

Compliance: Compliance is a process that ensures that individuals are aware of the regulations, policies, and procedures that must be followed due to senior management's decisions. Compliance is the evaluation of what is actually happening in the organization. The results will be compared with management's objectives, policies, and regulatory requirements. External factors, such as regulations, standards, and industry best practices, have to be followed and integrated. Organizations may need to respond to a variety of regulatory bodies concerned with privacy, information security and organizational trustworthiness, from the Securities and Exchange Commission to the European Union.

2.3.1 The »++« Additions to the GRC: Intensity Levels, Engagement Management, Ethics and Culture

SEEF Intensity Levels: Intensity levels create a risk-based view between engaging parties during a Social Engineering engagement. Intensity levels range from 1 to 12. Level zero represents the lowest risk, and level 12 carries the most risk. Chapter 4 discusses the intensity levels and how to use them. Management must adjust the intensity to the specific environment and engagement it is undertaking.

Engagement Management: Engagement management is a specifically designed method for Social Engineering engagements. The method contains specific risk gates that are especially important for Social Engineering engagements. It contains a start-to-finish client- and job-risk assessment. This means that, through the entire engagement, the client and the engagement will be observed for significant changes in the risk profile. Other risk gates include client selection and acquisition, scoping based on intensity levels, attack vector development and approach selection method.

Ethics: Ethics involves creating a reputation for honesty, fairness, respect, responsibility, integrity, trust and sound business judgment. Illegal or unethical behavior should not compromise the company's principles. A company's ethics is the sum of the ethics of every individual worker, so everyone is expected to adhere to high standards of personal integrity. The goal is to prevent conflicts between personal interests and company or client interests. Bribing, kickbacks and other similar activities intended to influence business outcomes are unacceptable. In our experience, it is advisable to have clear regulations on the topics of accepting gifts and using gratuities, fees, bonuses or excessive entertainment to attract or influence business activity. From the perspective of risk management (especially that of reputation risk) and in terms of the law, if a company has not regulated these topics, it is walking in a minefield. Ethical standards and regulations determine SEEF's intensity levels and engagement management, which define the ethical boundaries SEEF sets for itself.

Culture: Culture can refer to either an individual or a business. Customs are also part of culture. For instance, greeting someone with a handshake is a custom that differs from location to location and from audience to audience. Culture is reflected in people's behavior. People can adapt to different cultures, but they tend to be rooted in their own culture. People often fall back into the cultural schemes or customs they have experienced the most. Violating or disregarding cultural customs can be as bad as breaking the law, and it can build up hostility. Culture can play into a social engineer's hands—for instance, in a culture in which authority is not easily challenged. However, it can also cripple a Social Engineering approach that doesn't consider the context in which the Social Engineering engagement is executed.

The above-described GRC++ method and the predefined intensity levels will be fine for over 90% of engagements. The intensity levels are based on best-practice standards and what is commonly acceptable in the business world. You can apply these levels directly in the US, Europe and Australia. The framework has also been built with flexibility in mind, which means that parts of the framework can be tailored and adjusted to your specific situation. Note, however,



Figure 3: Governance, Risk and Compliance (GRC)++

that if you must deviate significantly from the GRC++ or the intensity levels, such as for highly political or religiously driven engagements, you should consider not engaging at all. My recommendation is that it is better to refuse these types of jobs.

2.3.2 Intensity Levels

Intensity levels are part of the unique methods SEEF has developed for creating a risk-based view between engaging parties, individuals or a company itself during a Social Engineering engagement. The intensity levels are represented by a table of 12 steps, ranging from levels 1–12. Level 1 represents the lowest level and carries the lowest risk and the least possible consequences. Level 12 is the highest level and carries the most risk and the greatest possible consequences. The intensity levels are benchmarking levels and express the risk and possible consequences associated with a task or approach.

The intensity levels have been pre-grouped into risk groups based on traffic-signal colors (red, orange, green). There is an additional group for intensity levels 10–12. We have seen Social Engineering engagements and attacks at this level (forms of industrial espionage and cyberwar, for instance). From a professional and commercial perspective engaging in activities at this level is not sensible. The black group (intensity levels 10–12) is there for completeness but no methods, tools or instructions will be shared about this level.

Green Levels

Intensity levels 1–3 are characterized by a low risk appetite and low consequences, and are considered mostly to be within legal boundaries. The group itself is divided into three distinct levels.

Level 1 Green: Within legal boundaries, non-invasive, based on open source intelligence (OSINT), publicly available sources, overt operation.

Level 2 Green: Simple tasks or engagement, local or national scope, standard corporations (no politically exposed or VIP targets).

Level 3 Green: Preservation of a person's/ company's integrity.

Signoff and approval, possible consequences and techniques used

The engineer or specialist on the engagement can execute assigned tasks on his own after his tasks have been released for execution. Use of your own staff is allowed. Simple tasks (i.e., OSINT) can be outsourced. Information can be bought or sourced externally. The externally bought or sourced Information must be collected based on the same principles (i.e., intensity level) as defined by the scope of the engagement or task. This means illegally obtained information or information acquired above the designated intensity level cannot be used. Risk has to be assessed by the engagement manager.

Orange Levels

Intensity levels 4–6 are characterized by an elevated risk appetite and higher consequences, and are not always considered to be within legal boundaries; some approaches may be considered misdemeanors. The group itself is divided into three distinct levels.

Level 4 Orange: Invasive, intrusive, medium complexity, involving international or well-known companies or individuals.

Level 5 Orange: Ethically questionable from a professional or personal point of view.

Level 6 Orange: Occasional risk of Illegal activities (misdemeanors), possible legal implications not en-

tirely known.

Signoff and approval, possible consequences and techniques used

Tasks have to be signed off by the project manager responsible for the engagement. Identified risks have to be mitigated or respective assurances collected. Additional requirements for engagements at this level include: official formal signoff by the client's management; definition of a contingency plan; compulsory team instruction about the identified risks and tasks within the engagement; compartmentalization of tasks and splitting of risks; staffing only with risk-averse senior and experienced resources; constant monitoring of status and progress; legal advice required and mandatory; engagement to be approved by two company directors.

Red Levels

Intensity levels 7–9 are characterized by a very high risk appetite, severe consequences and are considered to be outside legal boundaries. The group itself is divided into three distinct levels.

Level 7 Red: Invasive, intrusive, highly complex engagements or tasks; international scope, high-profile political or medially present organizations or individuals.

Level 8 Red: Coercion, unethical, risk of collateral damages.

Level 9 Red: Illegal activities (felonies), active crime, bodily harm.

Signoff and approval, possible consequences and techniques used

If during an engagement you reach higher levels, try to mitigate immediately to acceptable levels. Stop continuation of risk-loaded tasks. Immediately stop the engagement if necessary. Offer active support to investigating authorities, as you are obligated to report discovered crimes. Compartmentalize engagement from company resources and use outsourcing contracts for execution.

Black Level

Intensity levels 10–12 are characterized by a limitless risk appetite and devastating consequences, and are considered way outside the legal and ethical boundaries.

Levels 10 - 12 Black: Highly illegal activities including treason, breach of international law, possible death sentences, cyber warfare, industrial espionage, and loss of lives.

Signoff and approval, possible consequences and techniques used

DO NOT ENGAGE!

On the following page is a sample SEEF intensity-level table. It probably works for most of your engagements. It has been adjusted to American standards (misdemeanors, felonies, etc.). This table can be tailored to your specific needs or context in terms of culture, location, applicable legislation, GRC++, ethics, and so on.

2.3.3 Why use SEEF intensity levels?

The SEEF intensity levels can be applied and used in many different contexts. They are first and foremost a communication tool. During engagement planning (scoping, attack vector development) or field work, everyone can refer to the intensity levels as a mean of risk management. This establishes a common ground to ensure that everyone stays within the agreed methods and risks. Communication is very easy with the help of this reference.

The SEEF intensity levels can be applied in three different areas.

- Personal
- Engagement
- Company

On a personal level you might align yourself with the SEEF intensity levels in different ways.

- As a freelancer you might decide not to engage in activities above level 3.
- From a personal ethics point of view you might not work on level 6 engagements.
- During »in person« physical engagements you may not execute level 5 tasks.

From an engagement perspective the following can influence your risk behavior.

- You may limit the intensity levels since the client only allows methods associated with level 3 and lower.
- The intensity levels are a part of the scoping and agreement for a job.
- For attack vector development (AVD), the necessary intensity levels are predefined.

On a company level you can also define intensity levels.

- Defining company policy to engage only in level 1–3 activities.
- Mandatory use of external resources for level 7–9 activities.
- Executing international engagements on level 1only.

In the field we use the intensity levels to reflect on the tasks we are executing to benchmark ourselves according to this standard. Fieldwork often requires adjustment to the approach and the methods you use to achieve a set goal. In these moments of adjustment, things can go very wrong. You might overstep a line without bad intentions or you can bring yourself or your employer in a tricky situation with serious legal or other consequences.

How to use it

- Set and agree on the SEEF intensity levels for scoping and engagement development;
- Get the scope and Intensity levels signed off by the client;

Level	Risk Appetite, consequences	Signoff, approval, comment
1	Legal, non-invasive, OSINT	Engineer or specialist on the engagement can execute assigned tasks on his own after his tasks have been released for execution. Use own staff. Simple tasks i.e. OSINT can be outsourced. Risk to be assessed by engagement manager.
2	simple, local or national, standard corporation	
3	preservation of person/ company integrity	
4	Invasive, intrusive, medium complexity, international, well known corporation	Tasks have to be signed off by the responsible project manager of the engagement. Risks have to be mitigated or respective assurances collected. Official formal sign off by the client management. Definition of a contingency plan. Instruct team about identified risks. Compartmentalize tasks and split risk. Only Senior resources. Constant monitoring of status and progress. Legal advice required and mandatory. Engagement to be approved by two company directors.
5	Ethically questionable	
6	Occasional risk of Illegal (misdemeanours) activity, legal implications not known entirely	
7	Invasive, intrusive, highly complex, international, high profile political or medially present organization,	If during the engagement you have been reached higher levels try to mitigate immediately to acceptable levels. Stop continuation of risk loaded tasks. Immediately stop the engagement. Offer active support to investigating authorities. Obligation to report discovered crime. Compartmentalize engagement from company resources. Use of outsourcing contracts for execution.
8	Coercion, unethical, risk of collateral damages	
9	Illegal (felonies), active crime, bodily harm	
10-12	Highly illegal, treason, breach of international law, possible death sentence, cyber warfare, industrial espionage, cost of lives	DO NOT ENGAGE! DO NOT ENGAGE! DO NOT ENGAGE!

Figure 4: SEEF Intensity Levels

- Do not work on an engagements where no intensity levels are set or defined;
- Declare your own personal intensity levels;
- Maintain full transparency on the intensity levels defined; and
- Adjust the intensity level table as necessary based on your context or the specific requirements of the engagement or task at hand.

Tips

Take the intensity levels table with you when you meet with your client for the first time. You can use the table to focus your scope and eliminate misunderstandings during formal or informal discussions of the engagement, project or task assignment.

2.4 Approach Selection Method (ASM)

Social Engineering Engagement Framework (SEEF) approach selection method (ASM) allows you to plan the most efficient, effective and economical approach for your engagements. ASM allows you to factor in a multitude of attributes (i.e. time, money, chance of success, skill levels, stealth factor, complexity, and intensity level). Additionally, each selected approach will be graphically modeled based on the principles of the selected approach. Certain approaches or tasks can only be executed once but then your cover is blown; others can be repeated multiple times and some need to be specifically sequenced.

What is it?

Approach selection method (ASM) is one of SEEF's uniquely developed methods. As a social engineer you have the choice of how you will achieve a specific goal. There are many different ways to skin a cat, as we say. This means you can choose many different ways to achieve your goal. Approach selection method (ASM) is here to help you with that process. If your goal is to distribute a memory stick with a malicious payload, for instance, you can choose from among different ways of going about it:

- Place the memory stick in the employee parking lot.
- Drop the memory stick at the reception desk.
- Place the memory stick in the cafeteria.
- Place the memory stick on an employee's desk.
- Send a letter with the memory stick to a selected employee.
- Personally insert the memory stick into an employee's PC.
- Encourage an employee to try out a new game on the memory stick.

Each approach probably has the same outcome and will achieve your goal. However, each approach also has a different impact and carries different risks with it. In professional Social Engineering engagements you have to consider constraints and success factors as well as costs and other socioeconomic factors; there is a hell of a lot to think about. In the end it's about how you can achieve a specific task, with a guaranteed outcome, in the most elegant and economical way. One approach may be more costly to execute but the chance of success is much higher, while another approach costs less but has a lesser chance of success. Maybe you may choose tthe approach that is the most

stealthy but is also very time and labor intensive. The problem you are facing is, how do you select the best or right approach? Based on what criteria? What is the most effective, efficient and economical approach to achieve your goal? ASM will help you to answer exactly these questions.

3 Attack Vector Development (AVD)

Attack vectors are the bread and butter for social engineers. The success of an engagement is based on carefully selected attack vectors. For standard Social Engineering engagements, you can use well-known Social Engineering attacks or variants thereof. They work well and have been proven to be successful over time. If you are executing highly complex Social Engineering attacks on an international scale, you will need to develop very sophisticated attack vectors. You need personalized attack vectors. These attack vectors are developed on the specific intelligence about the target.

As experienced professional social engineers ourselves, we could not find a method for developing high-quality attack vectors. This is why we decided to develop our own methodology for attack vector development (AVD). A Social Engineering attack vector incorporates a multitude of attributes. If you have created an attack vector to be used in the USA, it might not work in Europe or Asia. Culture also has a significant impact on attack vectors, and we are also referring to coporate culture here. What is acceptable in one culture might be unacceptable in another.

The attack vector development method helps you to become more aware of those make-or-break differences in successful or unsuccessful attack vectors. AVD either uses predefined data (information) for the development of the attack vectors or creates its own data during the AVD development stage.

AVD depends on quality information (intelligence). The collection of Information is a very important step of the attack vector development process. The collection process in itself is a huge topic and not part of the AVD method. You can have different approaches for information collection. You have the choice to either collect the information yourself (make) or buy the required information. There is also a differentiation between an active or passive collection process. Well-known methods for information collection can be applied or selected for this task (OSINT, PSYCHINT, SIGINT and Recon).

After the collection process, the information must be documented in an appropriate way. Documentation ranges from verbal-only instruction with no traceable paper trail to file-based reports or workpapers. For the attack vector development, it is important to know whether the information is fact-based or what we call intelligence-based. Fact-based means that the pure facts are documented and described. Intelligence-based means that fact-based information has been enriched with intelligence or qualification. In the AVD, it is essential to know if the information source is someone's interpretation of the facts or if it is raw information. Examples for intelligence-based information are: psych. evaluations, personality tests, job qualifications, endorsements, SER maps (social and emotional relationship maps) etc.

The results of the attack vector development are carried over to the approach selection method (ASM).

We differentiate between two general types of attack vectors. These are generalized categories where most of the Social Engineering attacks fall under.

- Person-based (physical) or
- Technology-based (cyber)

Person-based means that an actual person is required to execute the attack vector. The person himself can either act onsite or remote. An Onsite person-based attack vector includes, for instance, following someone into a building without having access yourself (called tailgating). A Remote person-based attack vector , for instance, might include calling someone and acting as an employee (called impersonation) to elicit valuable information (known as phishing calls).

Technology or cyber-based attack vectors include all sorts of technology, gadgetry and software. This ranges from spy technology such as bugs, cameras, wiretaps to Trojan horses, malware, geolocation tools, keyloggers, phishing emails, malicious payloads etc. There is a never-ending supply of tools and technology. The technology or cyber-based attack vectors can be remote or location-based. Remote means that a phishing email will be sent remotely to the target's pc, laptop or mobile phone and executed accordingly. Distributed denial of service attacks DDoS are also remote-based attack types. Local technology or cyber-based attacks include the planting of bugs, cameras or keyloggers at a physical location.

Aside from the attack type (person- or technology-based), we use the so called attack vector principle for the development of attack vectors. This principle is the heart of the attack vector development. What principle do you choose as an attack vector? If the client wants a standard phishing attack to test the response of his or her staff, then you can choose a standard engagement based on standard or well-known attack vectors. But if your task is to social engineer the executive members of the Blackhat conference, then you might put a bit more thought into the attack vector development.

Fig.6 shows a table with selected attack vector principles ranging from standard attack vectors to highly sophisticated attack vectors in relation to development costs and effort to develop versus the importance of task or engagement.

During attack vector development, you must also consider the usual project constraints. The usual constraints are restrictions applied to your attack vector

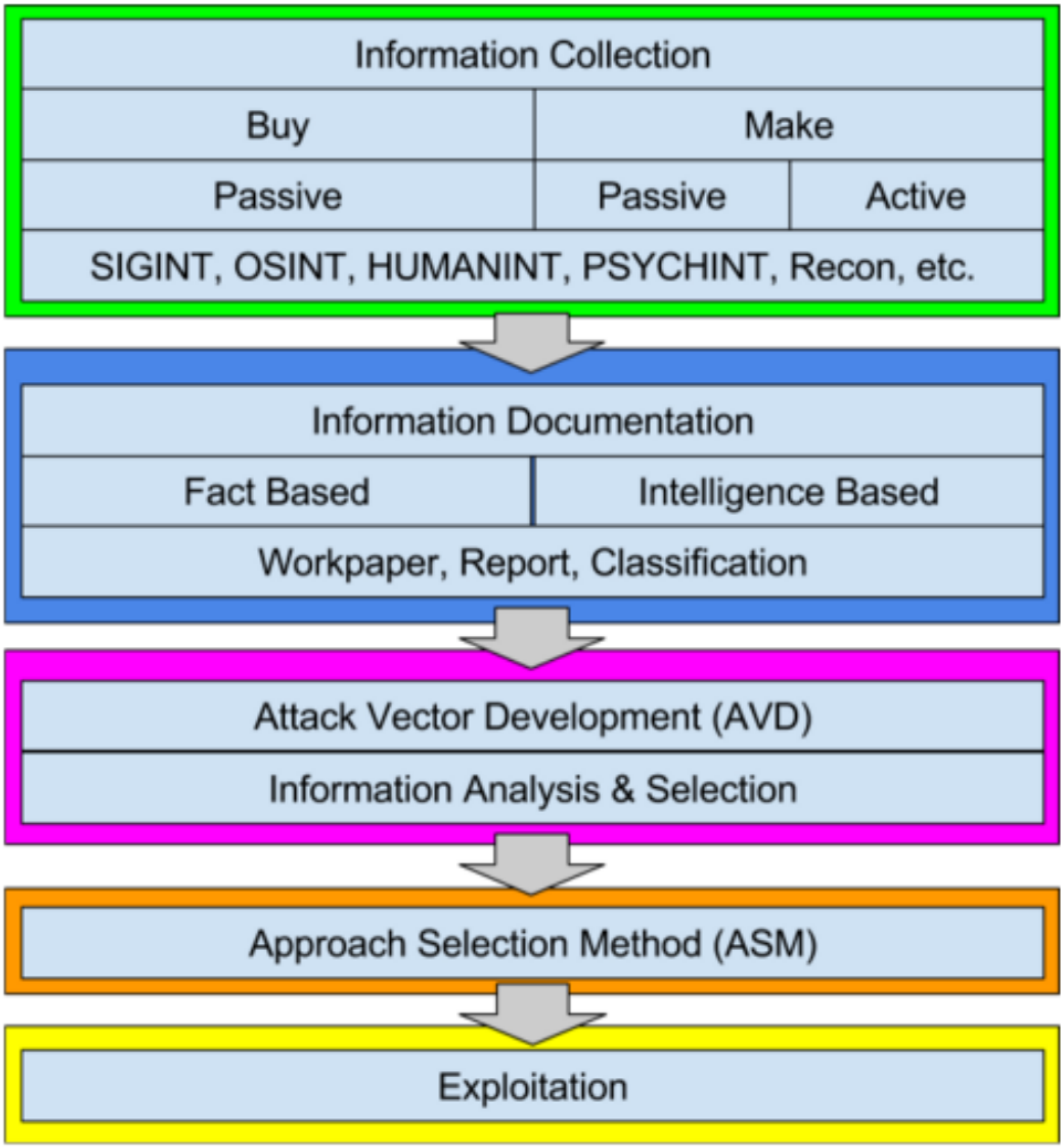


Figure 5: Attack Vector Development (AVD), Process

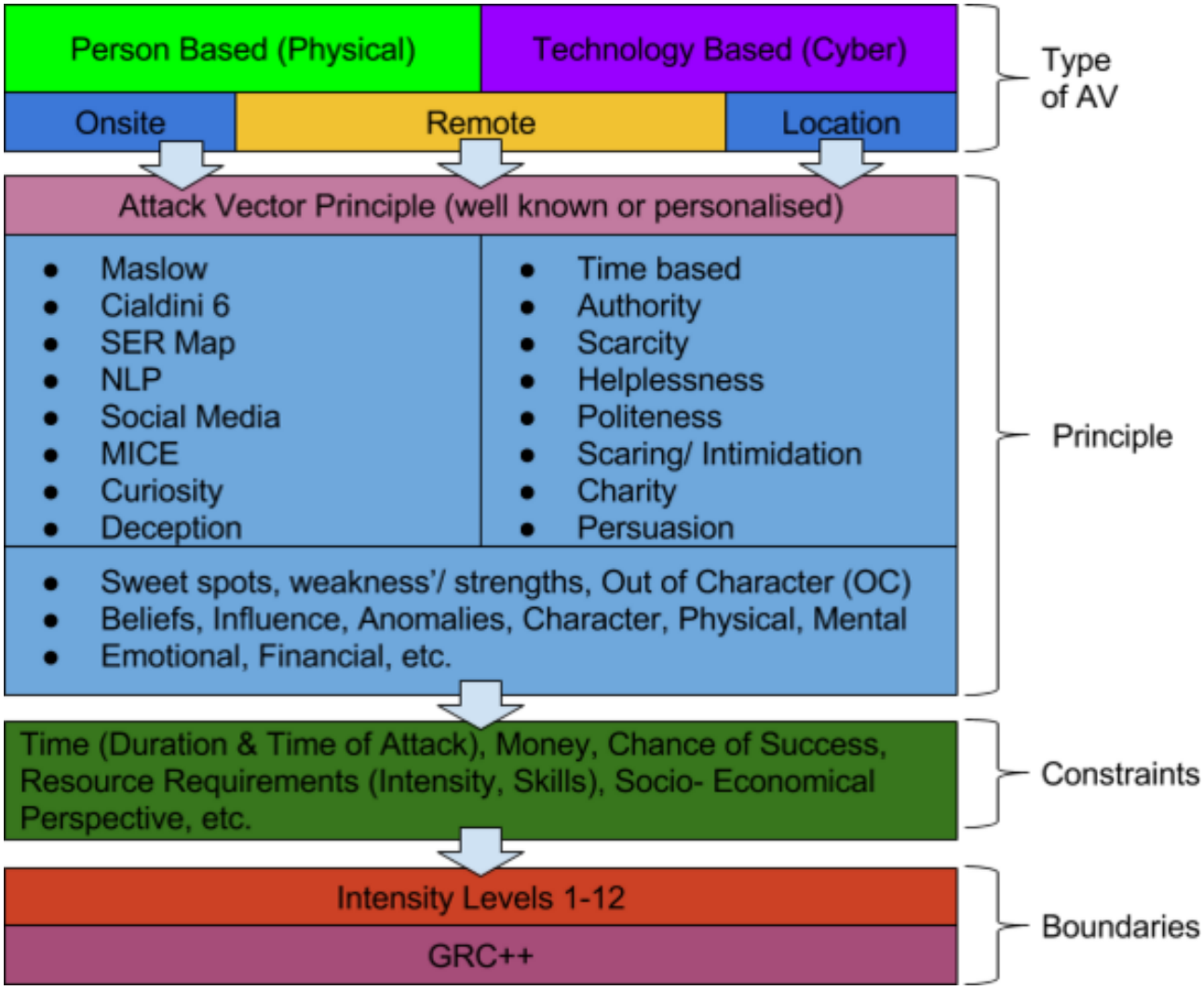


Figure 6: Vector Development (AVD), Context

development, either from your client or the project scoping; for instance, the budget you have available, the resources selected or a specific skill that you need but is not available. If you want to develop an attack vector based on psych profiling, then you might need an experienced profiler or a psychologist to help you with this.

Complex SE attacks require an orchestration of different tasks and techniques. A single attack is usually a means to an end. Social Engineering is often used in cyberattacks for a specific goal such as obtaining passwords, for example. This is also the reason why it is sometimes difficult to spot or correlate isolated events. Attacks follow a specific sequence. Correct and appropriate sequencing is one of the most important tasks in attack vector development. Attack types vary during an attack; this means that a person-based attack can be followed by a technology-based attack and then a cyber-attack and vice versa.

Attack vector development can be very time, resource and cost intensive. For less important engagement or tasks, you will typically rely on standard or well-known SE attack principles. Standard or well-known SE attack principles use generalized knowledge about people, cultures and behaviors. Generalized means that the principles or methods described will apply generally to people, cultures and behaviors. It could be that your generalized attack might not work in the context of your Social Engineering engagement or target.

3.1 Standard or well-known SE attacks

List with the standard or well-known SE attacks:

Baiting

- Description: Baiting is the process of distributing a bait, usually in the form of an object for the target to obtain. Baiting typically includes the use of electronic gadgets as baits, such as memory sticks, CDs, shiny keyboards, iPads etc. But it could also be something more substantial like cars, trips etc., depending on your budget. The bait itself contains a malicious payload such as a Trojan or similar malware to gain remote control of the target's hardware or obtain information.
- Intensity Level: Baiting can occur in a non-invasive way, and if carefully planned, it can stay within the intensity level of group green (levels 1-3). If baiting is going south, then you might increase the intensity levels up to 4 and break more federal laws and risk lawsuits. See the Computer Fraud and Abuse Act (CFAA) for more information.
- GRC++: The risks include losing the bait to a non-target or violating laws in regard to distributing malware. Unaccounted baits present an inherent risk to you and your engagements. If the wrong person picks up the malware and data loss occurs, you could be held liable. Check if these risks are worth the effort or if there is a more elegant way of achieving your goal. If you're just testing the susceptibility of your targets to baiting, then you can combine baiting with phishing. Then you will install no malware on the bait and will rather use an awareness site for redirection. Be wary of the fine line between enticement and entrapment.

Impersonation

- Description: Impersonation is the method where a person represents her or himself under a false, fake or non-existent identity in order to gain access to a location, provoke actions (email from the CEO) or elicit information from a target.
- Intensity Level: Impersonation has the potential to quickly become uncontrolled, thus creating more than what is worth the effort.
- GRC++: Most social media sites and other websites have anti-impersonation policies or real name policies you might violate with impersonation. It is very difficult to impersonate someone without then going on to commit another offense (either civil or criminal) where false information and statements are eventually being made. Plan your engagement as a lawful and good faith exercise. It is perhaps illegal to impersonate a real person but not a fictitious one. Most state laws also provide that the impersonation of a public official is a criminal act. If taken too far and documents are matched with the impersonated persona, then heavy fines and legal ramifications occur. It is best to act as a representative in the name of the company engaging your services or act as the Social Engineering company that you are part of.

Tailgating

- Description: Tailgating is when an employee opens a door and then holds it open for others who are following him. This could include visitors without badges, tech personnel with spare parts or the passive acceptance of a uniformed worker. It can also occur covertly when a person waits after the door has been opened by a legitimate employee and then slips in or blocks the door just before the door closes.
- Intensity Level: Tailgating can be done within acceptable intensity levels (green, levels 1-3) if specified rules are followed. Tailgating can be done within acceptable intensity levels (green, levels 1-3) if specified rules are followed, which only include

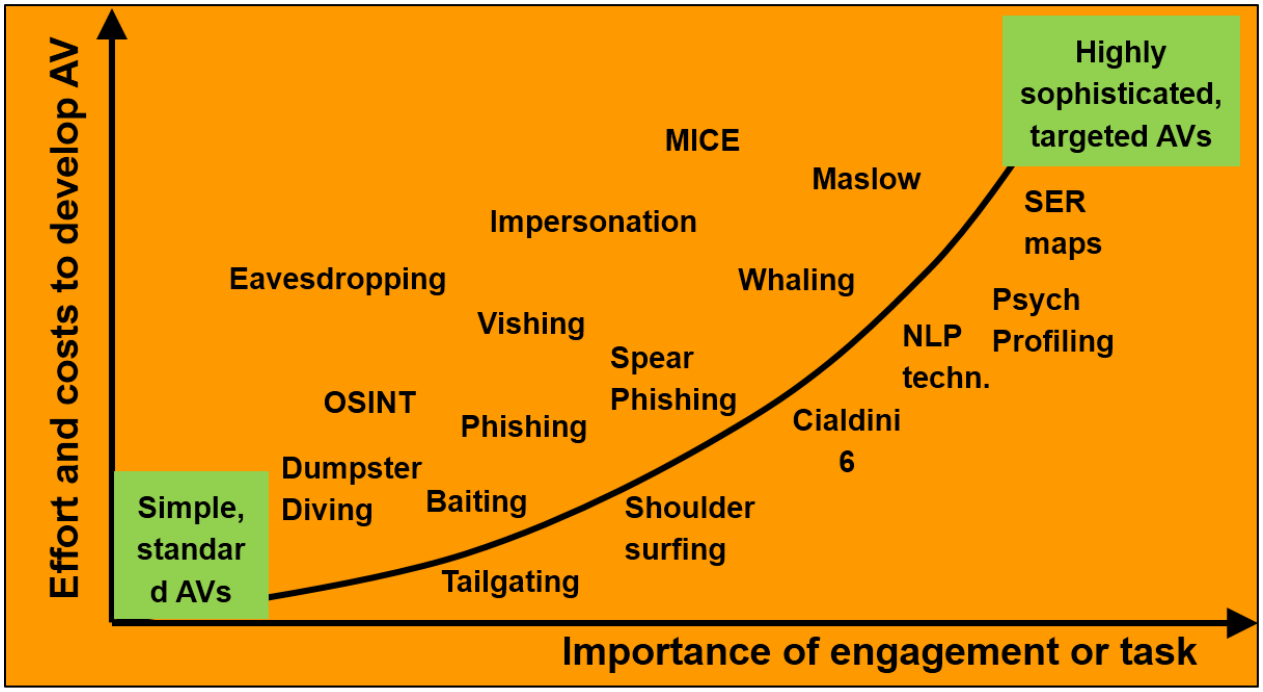


Figure 7: Attack Vector Development (AVD) Attack Types

working on politeness and speed without coercion, forcing entry or the stealing of access cards or credentials.

- GRC++: The »tailgatee« requires crystal-clear instructions about the behavior and boundaries he or she is expected to act in. There must be instructions about how, when and to whom the identity will be revealed. This could be planned as an open book exercise with the knowledge of the client and security staff. Or a closed book exercise with no none informed beforehand.

Dumpster Diving

- Description: Dumpster diving is the activity of searching through someone's garbage or trash in order to gain information. It includes standard household waste containers, landfills or small dumps.
- Intensity Level: Dumpster diving can be done within acceptable intensity levels (green, levels 1-3) if rules are followed.
- GRC++: If a person discards trash, he or she has no «reasonable expectation of privacy« in the discarded items. It is very different when the garbage bins are in an enclosed area or on private property. You could risk trespassing or theft charges. You may not be asked to leave if the law appears to be on your side. Do not search for confrontations.

Phishing

- Description: Phishing is the act of sending emails to lure your targets to deceptive websites. The websites will appear to be from well-known or trustworthy entities that instead collect information for fraudulent purposes.
- Intensity Level: Phishing in a controlled environment and with the client's acceptance can be done within acceptable intensity levels (green, levels 1-3).
- GRC++: Engagements usually go south when the staff and appropriate internal key stakeholders are not properly informed or warned. Also, immediately following the phishing attack, the employees must have a central point for Q&As to raise their concerns and provide awareness education. The open book is the best approach, except for the test target group. IT, security and management should be aware of the planned exercise.

Shoulder Surfing

- Description: Shoulder surfing is the process of direct observation, such as looking over a person's shoulder, to obtain information. It works great with pretexting in crowded areas but can also be executed with binoculars or other vision-enhancing devices (cameras) from a distance.
- Intensity Level: Shoulder surfing can be done within acceptable intensity levels (green, levels 1-3) if rules are followed.
- GRC++: There is the risk of revelation of the

identity or counterintelligence of the social engineer.

3.2 Cialdini 6

Cialdini 6 stands for Dr. Robert B. Cialdini's book, »Influence: The Psychology of Persuasion,« from 1984. In his book, he describes six principles of persuasion. The principles play on fundamental human instincts and can be exploited by different means. These principles can be applied to marketing purposes and, of course, Social Engineering.

The principles are:

1. Reciprocation: If you give, you will receive in return.
2. Social Proof: When others are doing it, it's OK for me to do it too.
3. Commitment and Consistency: If I agreed, I will stick to it.
4. Liking: If it's like me, I like it.
5. Authority: If an expert (or authority figure) says it's true, then it's true.
6. Scarcity: If it is limited or rare, I want it.

How to create an Cialdini 6 based attack vector?

With these principles, you can create targeted attack vectors using Cialdini 6 as their base.

Attack Vector Development: Cialdini 6

Reciprocation Attack vectors for reciprocation can be developed around the principle of giving first and expecting a return later. Based on the attack type you select, gifting could include electronic gadgets, either tampered with, i.e., malware, virus, CCTV, bug inserted etc., or just the gadget without tampering. Be careful not to overstep the line based on the target's professional or personal boundaries. In the professional code of conduct of your target, some gifting may be seen as bribery. Small gifts for the help with a survey or small items during conferences as giveaways are totally OK. This could also include favors such as helping with a tight timeline or the development of a website. You can also provide free study material or access to resources that the target doesn't have. Reciprocation can go a long way and there is no use by date. It doesn't pay off immediately, so be patient. Let the target be thankful for your gift/help or favor and respond with, »No problem, I know you would do the same for me.«

Social Proof You can force your target into compliance with the help of social proof. Sources like social networking sites can act as social proof for the target. It feels normal to do the same when all others are doing it. Introduce yourself to the target (as whatever you want to be) through a friend. Refer to many others who have recommended him or her or have helped with the same survey you asked your target to fill out. If more than one source validates a task or action, the more likely a target complies. If more than one person tells you to evacuate a building, the more likely you will do it. The other department was very supportive with this task. Use terms such as »endorsed by,« »as used by« and the industry standard.

Commitment and Consistency People do not like to back out of commitments and promises. It feels incongruent to them. Try to elicit a verbal or written commitment to a task or an action. Can you do it? Place simple requests first so that the target can easily comply with and say yes to them. Then work from there and present the bigger requests. Is it OK if we follow-up with an online survey in a couple of days? Thank you for helping with this silly email problem, you are a great help. Can you also tell me why this remote access doesn't work?

Liking You went to the same conference as I did last year. It seems that you like Social Engineering as much as I do. I see you have the same certification as I do; that was really a pain in the ass to pass. Aside from work, I like hiking and participating in coy play. The last Super Bowl was awesome and my favorite team won. Without users, being an administrator would be a great job. I know what it's like to have 20 open tickets in our queue at 4 o' clock in the afternoon. I am more of a cat person than a dog person. Managers, admins, consultants, project managers, HR, IT, chief information security officers (CISOs) and the whole world suck; I feel you, mate.

Authority I want to consult an expert. This was verified by the specialists. The boss said he needs this urgently. I have direct orders. I am just following orders. It must be done according to management. I am just the messenger. I am the legal representative. I must have access to the premises immediately. The safety check is way overdue. We cannot risk failing compliance with the service intervals. You still have the old locks. I know from experience that they are the weakest link in all of the break-ins. The locks need replacement or a break-in could occur. The tax office is expecting the records to be delivered today. HR sent me to sort this out. Dress for success and use impressive credentials with matching business cards.

Scarcity Scarcity (whether actual or merely perceived) generates demand and compels your target to act quickly. Words like exclusive, limited, rare, VIP, platinum, etc. can quickly grab attention and provoke a reaction. »Limited offer, valid only today« creates a sense of urgency. You can also communicate that the offer is only valid until or your reply is required until »tomorrow / the following day.«

3.3 Money, Ideology, Coercion and Ego (MICE)

MICE is commonly used to respectively recruit spies to understand someone's motivation. MICE stands for Money, Ideology, Coercion and Ego. All these factors will help to recruit for your »cause.« If a single motivational factor is not enough, a combination of factors hitting the right mix for an individual will usually convince the recruitee. Carefully applied MICE can also be used for Social Engineering. It is a bit of a dated concept and has been surpassed by more modern and intimate recruiting frameworks. Aside from ego, none of the principles can be responsibly, and within acceptable intensity levels, used in professional Social Engineering. But - and here comes a big but - Ego is an amazing thing. In hacking history, for instance, there have been many pitfalls because of ego.

How to create an attack vector

The following list will give you some pointers for the development of attack vectors based on MICE.

Money Some recruiting works fine with money as the driving factor. This makes someone dependable on high-value assets like cars, watches and other pecuniary items. Money as a reward will motivate some but not all.

Ideology For instance people motivated by ideology committed to a belief system that places them at odds with their own government. Such Hacktivists f.ex. may risk everything for the »cause,« even imprisonment, for no payment or other form of compensation.

Coercion Can be used against unwilling participants. Blackmailing, loss of income or threats, i.e., potential consequences to their families and friends.

Ego This makes someone dependable on high-value assets like cars, watches and other pecuniary items. Nowadays, every security vulnerability or name must have its own logo. Think of the most recent ones such as Poodle, Shellshock and Heartbleed. The same is true for hackers, hacking groups and other entities. This name giving helps practitioners and researchers track and attribute tactics, techniques and procedures as well as ongoing campaigns back to the group or hacker. Why does every security researcher or hacker have to have a handle? This comes from the old days, yet the system handle in the IT industry is still in use as a representation of ones self, a signature item. You can see this in the care and thought put in some of these system handles. It is much like artists signing their work, or sprayers tagging a graffiti (including the artist's name in a creative way). Sometimes these system handles reveal more about a person's desires and wishes than talking with him or her for an hour. So pay careful attention to the system handles, chat names, nicknames or any other representation of a person in a different format. For some, you can truly say that their ego doesn't fit through the door :-).

Pattern recognition: This includes the use of a system handle, nickname or tag as a signature item; the large gap between confidence and abilities; opting-out rather than being flexible enough to find a compromise; wanting to make their own work look more valuable; and being easily offended.

Out of character (OC) behavior: Ego makes you pay too much at an auction. Create artificial competitive settings for the target. Use intentional wrongful attribution of success, ownership or credit to draw out the target.

Emotionally loaded areas: Let the ego override the target's sense of logic. Ego is like a pet, you need to feed it. Feed (enforce) the ego of your target but don't overdo it. Gently apply ego-strokes like flattery and approval.

Incongruency in personal and business life: Talk about your ideas as if they were their ideas. Then go on and seal it by saying, «I wish I'd thought of that.«

Strong or highly developed areas: n/a

Weak or underdeveloped areas: n/a

4 Neuro Linguistic Programming (NLP)

NLP was developed in the 1970s by Richard Bandler and John Grinder. Neuro-Linguistic Programming (NLP) is a method of influencing behavior through the use of language and other forms of communication. There are many different NLP techniques that can be used for many different purposes. Each NLP technique can be used by itself or in combination with other NLP techniques. In my view, the single most important technique is rapport building.

Rapport is the ability to relate to others by creating trust and understanding. It is the ability to see the others' model of the world and get them to understand yours. Successful interactions depend largely on the ability to establish and maintain rapport. A lot of decisions are based on rapport rather than detailed facts. You are more likely to buy from, agree with or support someone you trust and can relate to than from someone you can't.

You can also assess your target's dominant system for mental processing (sensory perception). You can do that by simply talking to the person and paying attention to what kind of words he or she uses. Responding using the same language gives him or her confidence that you have understood him or her and helps to establish rapport.

How to create an attack vector

Several techniques from NLP can be used for attack vector development in order to influence the behavior of your target. First and foremost, mastering NLP

techniques will boost your confidence in the interaction with your target as well as your observation and communication skills.

Rapport building

The professional social engineer understands that people have a reason for believing in their model of the world. As a social engineer, you will recognize that these beliefs carry powerful emotions within them. This demands that we are empathetic to these emotions. This does not mean that you have to share those beliefs. You should try to emphasize the similarities rather than the differences. Look for common ground. Get over your ego!

Discover commonalities as a mean for rapport building. Where are you from? What type of music do you like? Do you ski? Have you been to…? Commonality could mean a common enemy.

Matching and mirroring are powerful techniques. If someone raises his or her right hand and you also raise your right hand, this is called matching. If the person raises his or her right hand and you sit opposite to this person and raise your left hand, this is mirroring. You can match and mirror different aspects of the person you are engaging with.

- Posture
- Physiology
- Speech pattern (voice)

Posture: Does your target stand tall? Are the shoulders slumped or erect? Is he or she leaning to the right or left? What about the hands? Is he or she holding something, perhaps a clipboard, pen or a coffee cup? Observe how your target moves (fast, slow, energetic or lethargic). All of these traits can be matched and mirrored.

Physiology: You can you match the rate of a person's breathing. Observe how your target is breathing through the chest, abdomen or stomach and how deep. Check for facial expressions such as raising eyebrows and nodding/tilting the head. Nod back at the target to signal affirmation.

Speech pattern (voice): Figure out your target's voice pattern: pace, volume, pitch, tone and type of words. If your target is talking slowly, slow down. If he or she speaks softly, drop your volume. Use the same words to describe things and processes. Listen for key or power words and reflect them back during the conversation.

Matching and mirroring means a synchronized application of these techniques. But try not to match and mirror everything your target does. Mimic selected behaviors and delay mirroring and matching for a couple of seconds.

Be subtle and don't overdo it. If the target thinks you are mimicking him or her, he or she will be offended, perhaps thinking that you are mocking him or her.

NLP is a goldmine for a social engineer. The mastering of selected skills is a must.

5 Maslow's hierarchy of needs (Maslow)

Maslow developed the theory of the hierarchy of needs. Maslow believed that individuals have a set of motivation systems unrelated to unconscious desires or rewards. According to his theory, people are motivated to achieve to satisfy specific needs: Depicted in a pyramid, the theory groups different needs according to their level of importance.

The defined groups of needs in Maslow's hierarchy are:

- Physiological needs (including water, food and air – basic survival necessities)
- Safety needs (shelter and a stable job)
- Social needs (love and belongingness)
- Self-esteem needs (confidence and self-respect) and
- Self-actualization (characterized by self-understanding and full use of one's capabilities).

At the bottom of the pyramid are basic needs (food, water, shelter and sex). Lower needs must be met before the next level of needs are fulfilled. Safety needs are the next level of the pyramid, and although these needs are essential for survival, they are not as crucial as physiological needs. The third level in the pyramid are social needs, i.e., the need to belong and be loved. Social needs are all about the need for acceptance and companionship. The fourth level (esteem needs) is fulfilled when people are pleased with their achievements. Esteem needs comprise of anything that creates social recognition, accomplishments, competency, personal worth and self-esteem. At the top of the pyramid are self-actualization needs; self-actualization occurs when an individual achieves his or her full potential. Self-actualizing is mainly concerned with personal growth, and the person cares less about the opinions of others.

Physiological needs: air, food, drink, shelter, warmth, sex, sleep etc.

Safety needs: protection from elements, security, order, law, limits, stability etc.

Social needs: work group, family, affection, relationships etc.

Self-esteem needs: self-esteem, achievement, mastery, independence, status, dominance, prestige, managerial responsibility etc.

Self-actualization: realizing personal potential, self-fulfillment, seeking personal growth and peak experiences etc.

How to create an attack vector

Attack vectors based on Maslow's hierarchy of needs can be crafted based on the principle of meeting the unfulfilled needs of your target. In each category, you can have unfulfilled needs. First you must determine which needs could be unfulfilled.

In the category of physiological needs, you can evalu-

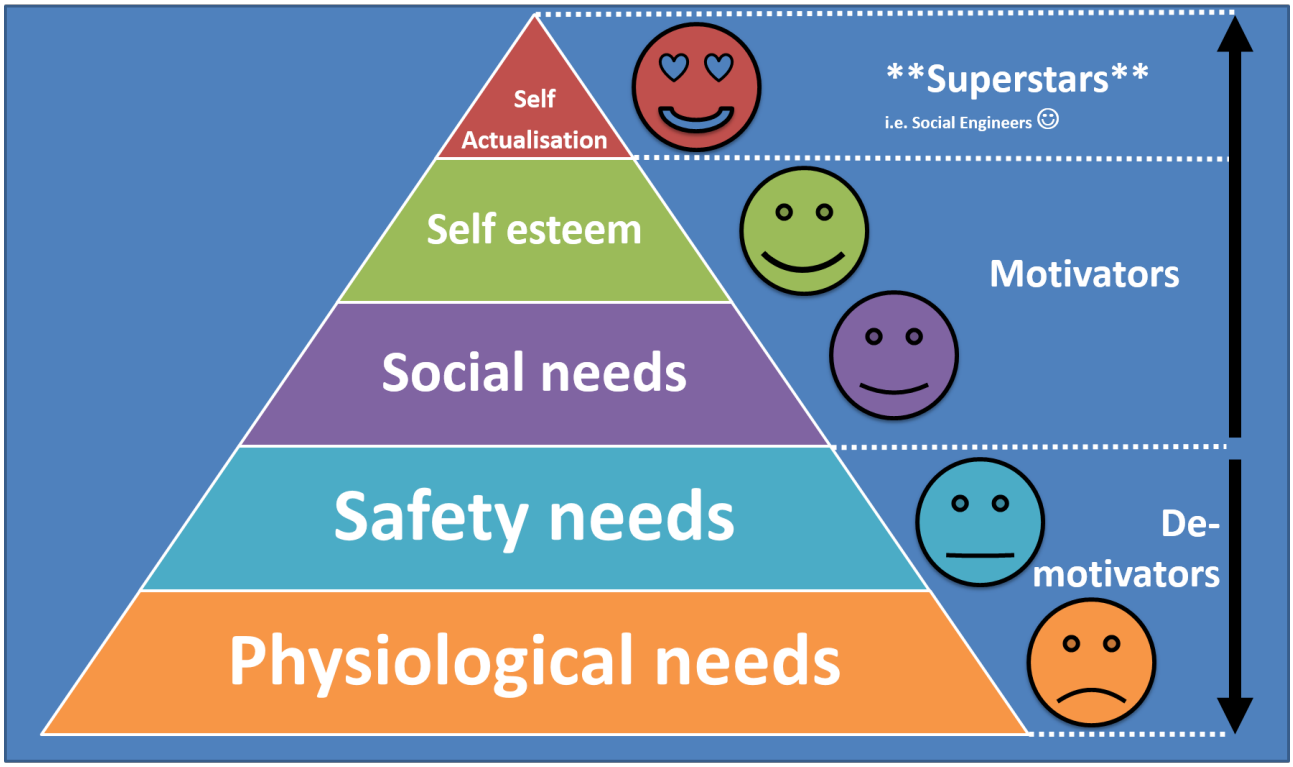


Figure 8: Attack Vector; Maslow Pyramid

ate the effectiveness of the following topics.

- Does the target have a cafeteria, vending machine or drinking fountain?
- Does your target get enough sleep?
- This category can also be described as «Only about me«.

For the safety needs, evaluate the effectiveness of the following topics.

- Where does your target work or live (safe and friendly location)?
- How is medical insurance or health care?
- Is the target's job secure? Any mergers, acquisitions or job cuts in sight?
- How is the financial stability or credit rating of your target?
- How are the wages and salaries (fringe benefits)?
- This category can also be described as «Me and my surrounding«.

When it comes to social needs, evaluate the effectiveness of the following topics (Me in context).

- How is the team spirit?
- Does the target have friends or colleagues?
- Is the target engaged in social activities?
- Is the target balanced and satisfied with his or her current situation?
- This category can also be described as «Me and the others around me«.

For the self-esteem needs, evaluate the effectiveness of the following topics.

- Is the target a respected member of the community or workplace?
- Does the target have responsibilities aligned with his or her capabilities?
- Is the target recognized for his or her achievements?
- This category can also be described as «Me, my achievements and my status«.

Finally for Self-actualization needs, evaluate the effectiveness of the following topics.

- Does the target have enough challenges?
- Is the target supported in his or her creativity or leadership?
- Does the target appear to be in a state of peak performance?
- Is the target fulfilled? (Achievement without fulfillment is not satisfactory).
- This category can also be described: «Who am I?«

If any of the above points is not fulfilled, then this is your leverage for creating your attack vector. You can use the unfulfilled needs as discussion points or as leverage.

Instead of using standard or well-known Social Engineering attacks, you can use personalized attack vectors. Social and emotional relationship (SER) maps are an example of a personalized attack vector.

6 Social and emotional relationship (SER) maps

Social and emotional relationship mapping is used to highlight a persons (or an organizations) social and emotional relationships. For the mapping, simple symbols and rules are used to graphically display the relationships. Social and emotional relationship maps are similar to genograms but differ in purpose, focus and depth. Some practitioners in personal and family therapy use genograms for personal records and/or to explain family dynamics.

Existing forms of documentation lack the social and emotional component. Organizational charts only represent the hierarchical structures of a given company and the people within this structure. For professional Social Engineering in the business context, a more refined representation of an organization or person is indispensable. As we all know from experience, there is a hidden informal structure behind any organizational chart. Some members of the management team might be best pals and others hate each other. Social and emotional relationship mapping (SER maps) helps you to establish and document these traits, mostly in transparent and non-documented information attributes.

This is how you read the map. Chris is the index person; he is 45 years old. He was married to Alice in 1999 and had an affair with Tiffany, age 20, in 2014. Chris' best pal is Bob. Bob has PTSD and is the same age as Chris. Alice is hostile toward Bob. Chris is focused on Claire, age 18.

How to create an attack vector

Based on the presented information from the social and emotional relationship map, you try to identify or evaluate the following attributes.

1. Pattern recognition
2. Out of character (OC) behavior
3. Emotionally loaded areas
4. Incongruency in personal and business life
5. Strong or highly developed areas
6. Weak or underdeveloped areas

7 Interpersonal Distance – The Concept of Space

As a professional social engineer, there are many things you need to know. You need to be versed in business matters, technology, culture and sociology—depending on whether you are a social engineer who likes the thrill of interacting with people or whether you are more of a tactician or strategist.

The concepts described will give you a basic idea and prepare you with the required knowledge to tackle those situations. Each situation and each new engagement can work out differently. This is the beauty of working with people: they are individuals and can react to the exact same situation in the same context in completely different ways! So you must be flexible, patient and motivated.

People react to other people or objects depending on their distance towards them. Usually we let friends and relatives or our partners closer to us, whereas we tend to keep our distance from strangers or dangerous things. Unwanted or unapproved proximity will trigger some sort of reaction (reaction zone).

There is a point of no return for every person; if you step into this circle then you will ultimately provoke a reaction. Maybe this is what you wanted, but maybe not; perhaps you just closed in too much on the target. For a social engineer it is of utmost importance to grasp this concept. You can have the best pretext there is, but if you mess up the communication and the interpersonal distance, you are done.

Stepping too close will shut you down and you will lose the trust of the target. If you do not maintain appropriate interpersonal distance, you cannot engage properly and will lose rapport with the target. In daily life there are four zones you can observe. Respecting and moving strategically between these zones let you »control« reactions to a certain degree.

Intimate space: Intimate space is the most important zone of all. It is reserved for a few people: parents, loved ones, children, and very close friends (depending on culture). Only loved ones or children are allowed to engage in this close physical proximity. Anyone who is not meant to be in the intimate zone and oversteps the boundary can make people feel threatened and cause physiological changes in their bodies.

Personal space: This is the distance reserved for social gatherings such as parties and friendly interactions, and is also used for private discussions. People will avoid entering a setting if you are engaged with someone at this distance. If you are trapped in a boring conversation, try moving a bit away. It will open up your space for someone to enter.

Reaction zone: If you approach someone in this zone you will provoke a reaction of some sort. Be prepared when entering this zone. Know you game-plan, be polite and smile. Prepare for a greeting; remember the person's name and read their nonverbal and verbal signs as they react to your entry. When entering this zone you need to make your move; entering and then immediately leaving the reaction zone (boomeranging out) is very awkward.

Social space: This space is reserved for strangers we have just met, acquaintances and anyone we interact but have not established a relationship with. This space is used for public and social conversations. Usually groups form at this distance. People can join the group or leave the group; it is a bit like a fish swarm. As a social engineer you can try to join the group and work your way forward to your target, or you can try to cut off your target from the group.

Public space: Public speakers and important figures use space to distance themselves from their audience.

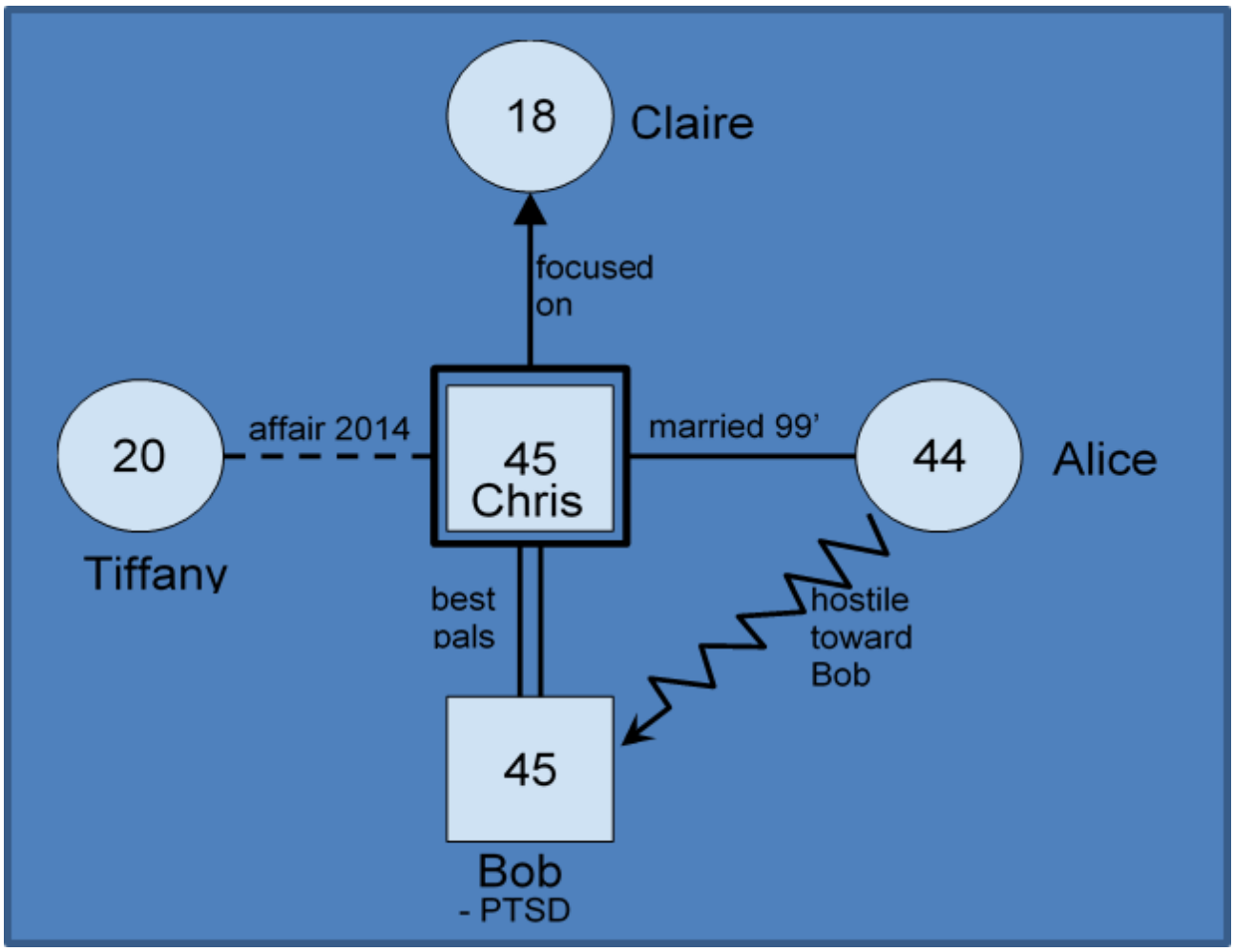


Figure 9: Attack Vector Development (AVD); sample SER map

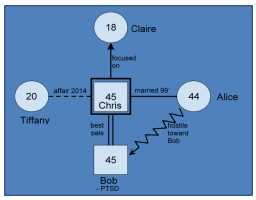
Attack Vector Development	SER map case: Chris, 45 years old
	***Pattern recognition:*** Since Chris had an affair with 20-year-old Tiffany, in addition to the focus he shows on 18-year-old Claire, there is a possible fixation on young women. Chris would eventually respond well to phishing emails with pictures of young girls and contact requests over social media based on young women. ***Out of character (OC) behavior:*** n/a Emotionally loaded areas: Alice, Chris' wife, is hostile toward Bob, Chris' best pal. Tiffany, Chris' affair from 2014, might hold a grudge against Chris and could act as an information repository. Bob could be used to gain information about Alice and ultimately about Chris. ***Incongruency in personal and business life***: n/a ***Strong or highly developed areas:*** n/a ***Weak or underdeveloped areas:*** n/a
Attack Vector Development	SER map case: Chris, 45 years old

Table 1: Attack Vector; SER map case study 1

Symbol	Meaning	Symbol	Meaning
	Male		Index Person
	Female		Pet

Symbol	Meaning	Symbol	Meaning
	Institution		Professional
	Incarcerated		Indifferent
	normal		Love
	Jealous		Manipulative
	Abuse		Best friends
	Divorced		Divorced reconciled
	Friendship		Focused on

Table 2: Symbols used in SER maps

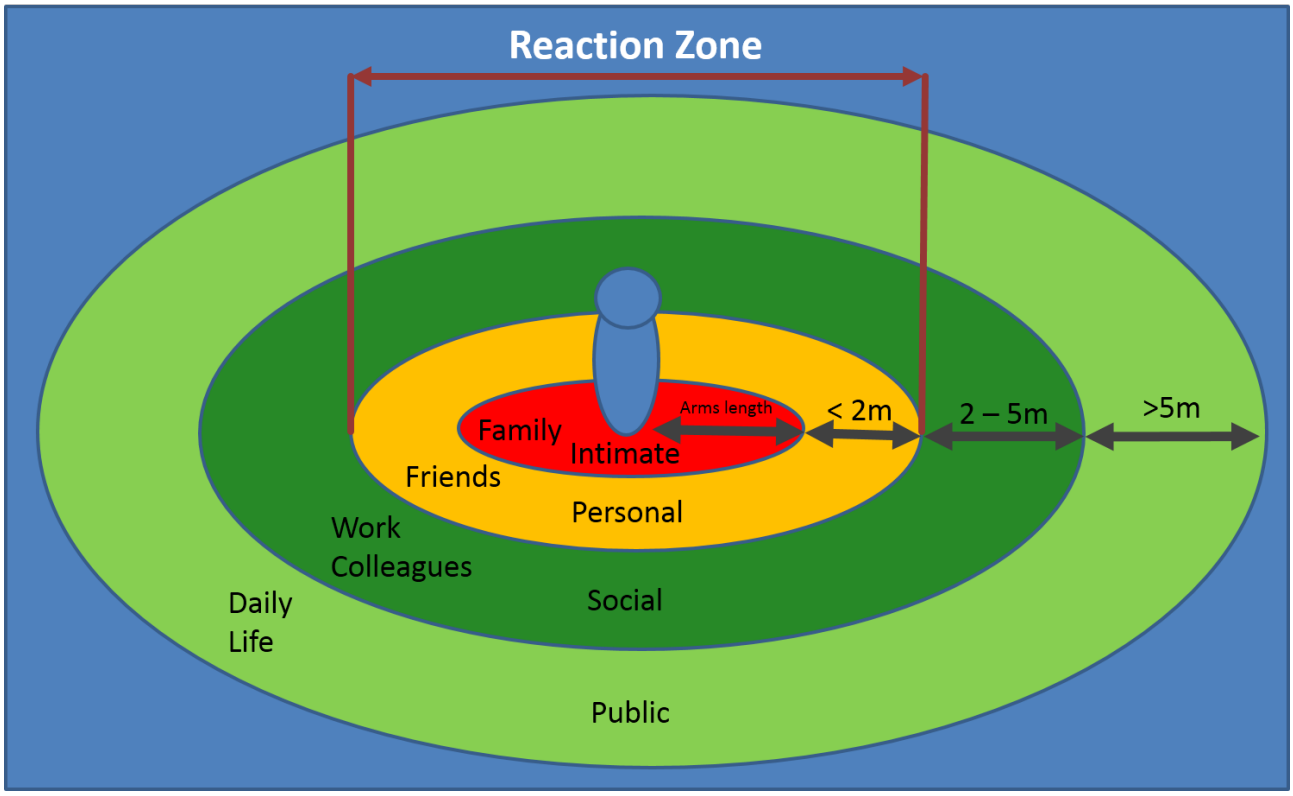


Figure 10: Interpersonal Distance the Concept of Space

This space can also be called the audience zone. It is used to address an audience or large group of people.

Interpersonal distance varies based on the culture or context you are in. By context I mean physical and geographical location, type of activity or mode of transportation. Here is an adjusted interpersonal distance map.

As a professional social engineer you need to be observant and recognize patterns—first and foremost, how people interact with each other and how the surroundings work.

Another important concept, aside from interpersonal distance, is the way you actually approach you target. In the business world it is appreciated if you don't sneak up on people and scare them because they are unaware of you approaching. Think of the various kinds of interpersonal distance as gates, where you must get verbal or nonverbal approval at each gate from the gate keeper in order to enter the next circle. Approaching too fast will trigger the target's fight-or-flight mode (what would you do if someone whom you never met suddenly runs towards you?). Keep a normal walking pace in your approach. If you see that the target—or, for instance, a security guard—is not aware of you, slow down and announce yourself.

You can do this by:

- Coughing;
- Dropping something;
- Clearing your throat;
- Standing still and then walking again; or
- Checking your phone quickly (taking a fictitious call or reading a message).

If this works then you should seek eye contact and approach as planned. Look for the reaction of your target when you approach. Try to spot whether they have identified you as a threat or as a friend. There is also a difference between men and women from the approach perspective, by which I actually mean the physical angle of your approach relative to the target. We differentiate three different zones:

- The backside of a person;
- The front side of a person; and
- The side of a person.

Women and men differ in the perception of these zones in relation to the angle and risk factor. Women tend to have a wider front where approaching is acceptable but the sides are smaller. Men tend to have a narrower front where approaching is acceptable, but also wider sides and the angle at the back is wider. The zones in the graphic are adjusted to a standard international business context.

In standard situations you will not be able to choose the angle of your approach, and there is a reason for this. A reception desk will not allow you to approach from the side or the back. The only way to approach is from the front, and this situation has been created by the construction and the setting of the desk and also its cultural context. If you try to access the space behind the reception desk it will be seen as a threat unless you have a plausible reason to enter. In addi-

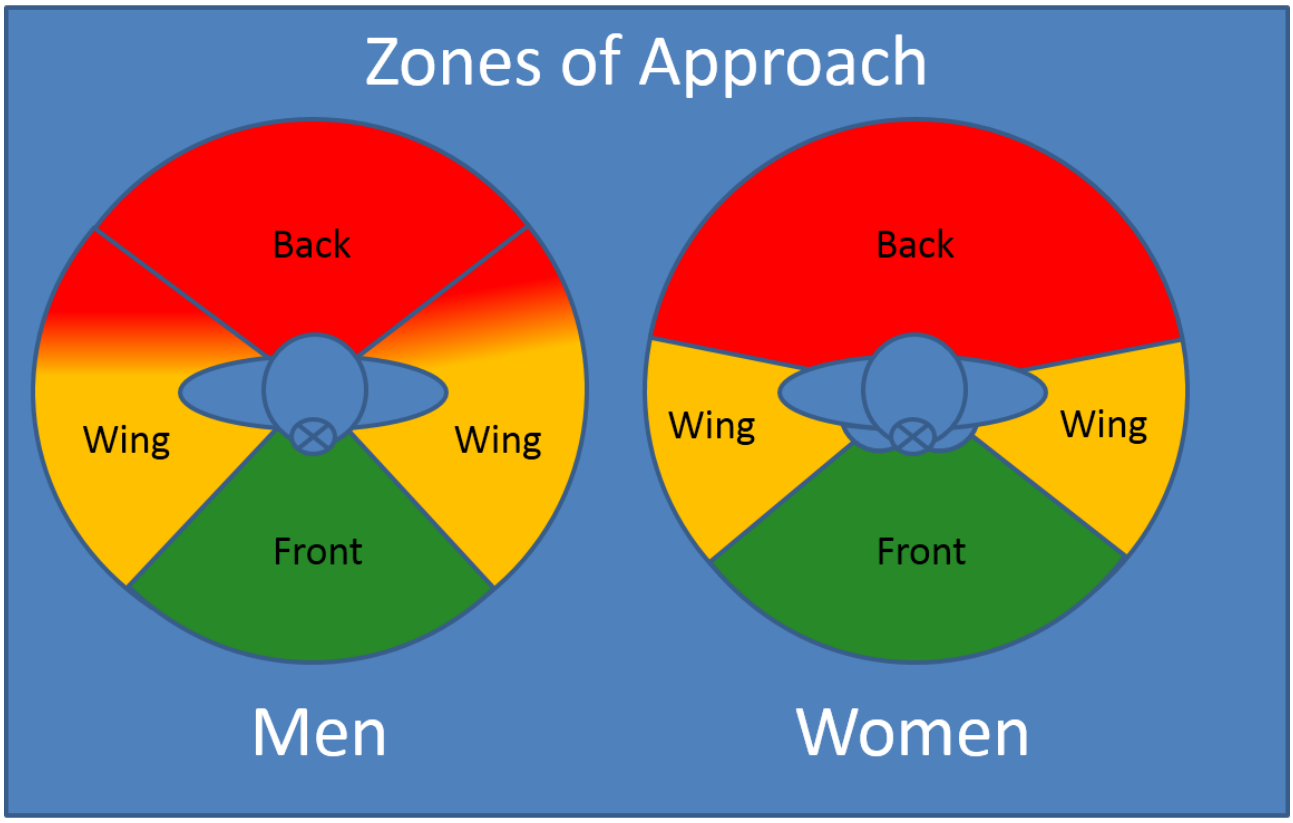


Figure 11: Zones of Approach; Men, Women

tion, you usually cannot see through the front of the reception desk. This gives the personnel a feeling of security but also prevents people who enter the reception area from seeing everything.

In different situations or contexts the zones of approach vary. Culture, location and other factors will influence the perception of approach. The zones of approach for military personnel in combat might look like the graphic below, highlighting nearly every angle of approach as a threat. A soldier might eliminate you from whatever angle you approach if you appear to be a threat.

The standard situation you will encounter most of the time is approaching someone at his or her desk. The combination of the two previous principles leads to the following graphic. In a business context, there is only a slight difference between genders.

As you can see, the optimal zone for approaching someone is from the front. Approaching from the side is also acceptable. However, behind a person, where you can't be seen, is a no-go zone. You should never approach someone sitting at a desk unannounced from the back. Of course, there is a bit of a problem in offices with cubicles where the desks are placed toward the wall. From the perspective of employees working in such a setting it is not a good feeling. They are never sure if someone is sneaking up on them. If you are seated like this and you cannot change the placement of your desk you might want to buy a mirror; with the aid of the mirror you can see what is going on behind your back. This can make you more comfortable sitting at your desk.

As a social engineer you will encounter this situation. In a setting like this it is important to give the person sitting at the desk the chance to react to your approach. You can artificially knock on the cubicle wall or you can call out the name of the person you are looking for. In applying this approach myself, I once approached a person in a cubicle from the front; I am tall enough to look into a cubicle - The person nearly had a heart attack when I approached him like that. This shows that you have to adjust your approach to every situation individually. There is no standard recipe. You have to decide between a potentially heart-attack-inducing approach and possibly embarrassing the person when you see the content on the screen as you approach her or him.

Over the years I have applied one simple rule that will get you through a lot in life—from not knowing which fork you use for the starter to greeting international guests at the airport. Demonstrate that you have social intelligence and good manners.

Observe: Observation is a critical skill for every social engineer. Through observation you can recognize the patterns of the context you are working in. How do people talk to each other? Are they holding the door for each other? How do they greet? Put yourself into an inconspicuous position and observe for a while. Read a newspaper or type on your laptop and skim your surroundings.

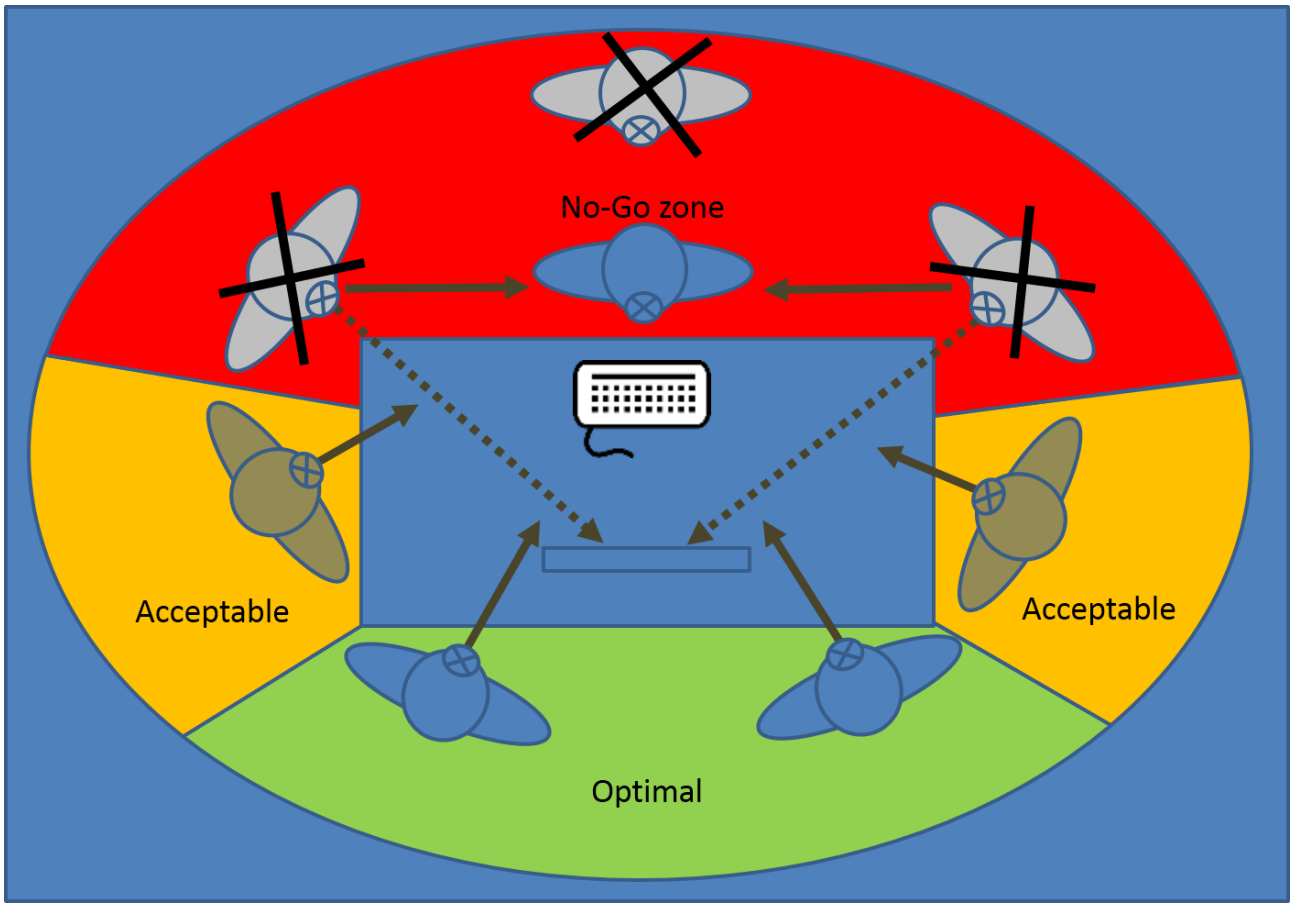


Figure 12: Zones of Approach; Desk

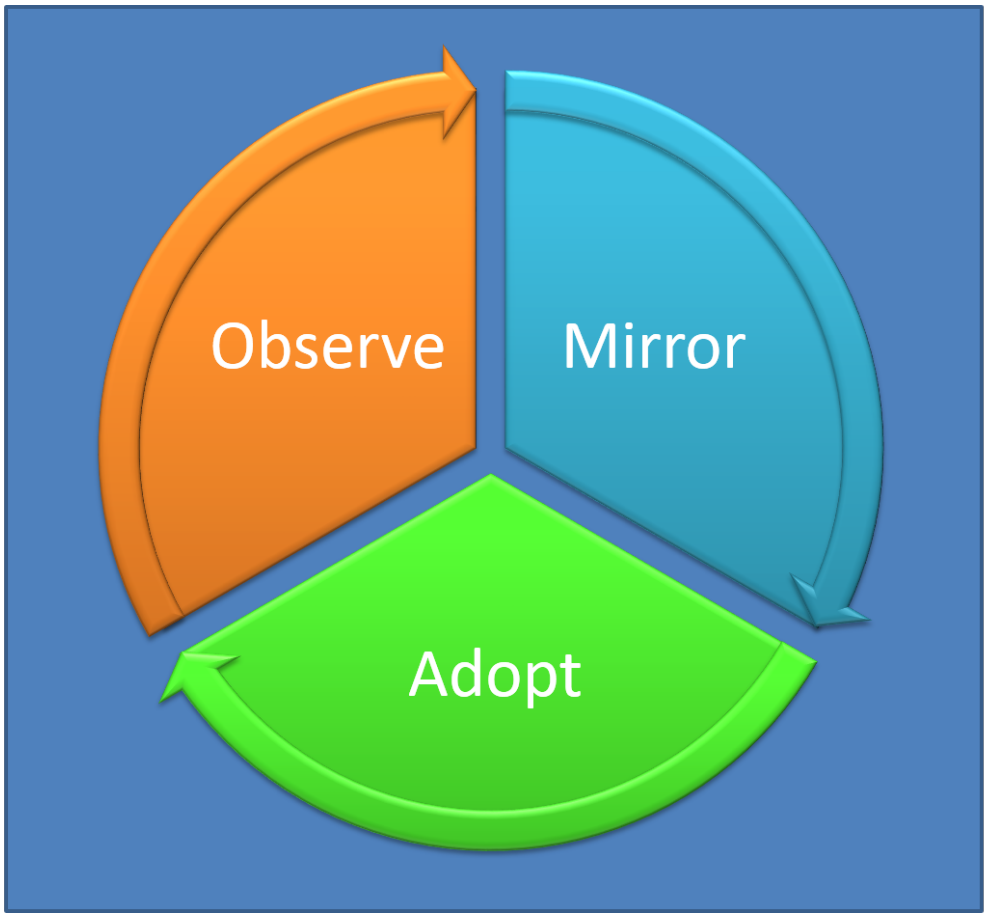


Figure 13: Observe, Mirror, Adopt

Mirror: When you have observed long enough then it is up to you mirror the behavior you have observed. Try to act naturally. Always be polite and smile. A great smile and empathy will take you a long way.

Adopt: Finally, when you get the hang of mirroring your surroundings, you can start adopting new behaviors. Adopting means going from conscious awareness of the wanted behavior to unconscious adoption of the wanted behavior (mastering the skills). Your mirrored skills need to become natural.

8 Target selection

One of the best sources for Social Engineering is active listening. A social engineer can gain so much information with just listening in on others' communication. Declared sources for the highest quality information are:

- Train transportation
- Airplane travel
- VIP and frequent flyer lounges
- Coffee shops and bars near your target
- Rental car office/desk
- Hotel lobby/bar and elevator
- Beach bar/club
- Disco/nightclub/rooftop
- Zoo
- Public canteen
- Tax office
- Post office
- Police station
- Beauty salon
- Conferences
- Public places like parks
- Cinema
- Shooting range
- Golf/ Tennis court
- Daycare center
- Hospital
- Dentist
- etc. (You name it.)

There is an abundance of great sources for listening in. One of the really great side effects for just listening in is that it is (mostly) legal. Stick to low tech; do not record the conversation and only make encrypted notes.

How do you select a good location for listening in? You can use different approaches for selecting a place for listening in. What are you after? Do you have a specific person as a target, a general company, or place in mind?

During my extensive traveling, I overheard many conversations. It is unbelievable how careless people are when it comes to verbal communication. After some conversations, I could have probably waltzed into that company with my newly acquired specific internal knowledge and posing a real threat.

The biggest problem from an educational and awareness perspective is:

»People do not apply the same care when engaging in verbal conversations as they would in electronic communication.«

Why is that so? There is a lack of guidance. In electronic communication, or working with files and data, we are just starting to learn how important classification of data is. Data must be classified in order to protect the data based on the well-known principles:

- Confidentiality
- Integrity
- Availability

People realize they must have passwords to protect their data, or they are using encrypted drives. Everyone knows a labelled HR document with the classification »Personal/Confidential« should not be posted on the cubicle wall next to the menu of the canteen. In verbal communication, though, we are far from this sort of awareness. Some conversations are like taking the confidential preliminary quarterly company results and placing them on every table at the frequent flyer airport lounge for everyone to read. You might shake your head in disbelief now and say: «This is insane. My employees and I would never do that.« Sorry to burst your bubble, but come to the airport with me, and I will show you first hand.

Remark: I exempt here people who are trained and have experience handling confidential and secret information. They know exactly what and how to say it. However, this is a very small percentage of the people out there. None of the business tycoons or larger corporations (the main targets for Social Engineers) is specifically trained and aware. What happens is, a person takes information and data out of a confidential, password-protected, integrity-checked, encrypted spreadsheet and broadcast it over the phone during a conversation. And all the security gadgetry in place for protection has just gone out of the window.

For verbal communication, you rely to 100% on the person's awareness, integrity and capability not to communicate confidential information. There is no technology that will help you doing this.

In the military and other sensitive areas, you specifically learn to speak code or at least use a coded language to transfer verbal information. You use abbreviations and code names for locations, so aside from



Figure 14: Target selection

technical protection, like encryption of radio or satellite communication, you actually encrypt information in verbal communication. This approach could also work for the private sector, but it needs a lot training and effort. No CEO would want to undergo communication training like you have in the army.

Because of this, we developed verbal masking. Verbal masking is an easy-to-learn approach for masking your verbal communication for business professionals. The method gives you tools and pointers on how you can verbally mask your conversation without being too awkward.

Verbal masking is an attempt to sensibly approach people and deliver some guidance in a standard situation. You can take this concept further and develop an internal code speak for instance.

Declaring position/ situation (full transparency): This is the most basic way of informing your communication partner about your current situation. If you observe your environment you will find that people are doing this automatically. Being transparent will give your communication partner the opportunity to decide what he can communicate and what not. Sometimes headhunters contacting you in the office on your business phone are able to pull this is off quite nicely. For instance, it might sound like this:

You are receiving a phone call: »Oh, hi Peter; haven't heard from you in a while! How are you?« Response from Peter. Then you say, »I am very well, thanks. I am in the office right now, with Bob and Alice and have you on the speakerphone.«

Try to declare your position/situation in relation to its sender-receiver relationship (1 to 1, 1 to many, many too many) and the space, place, location and situation you are in. This gives Peter the opportunity to adjust his communication style accordingly.

You are making a phone call:

1) »Hi Daniel, it's me Obama. I am in the square office together with Mustafa See I A and Francois EnSA. I put you on speakerphone so everyone can hear you.«

2) »Hi, Obama here. Can we talk in private?«

3) »Hi, Obama here. I'm alone right now but am running a live Twitter feed and have to check my shares' prices occasionally. and the chat with my wife is running hot.«

»Declare your situation actively and transparently. State your situation in relation to space, place, location and your sender or receiver status.«

What if you cannot do this? There are situations where you cannot steer a communication this way. Then you try to…

Covertly signal your communication partner (sender or receiver) through a sharpturn or code word that you are not able to talk freely«

A sharp turn means a change in the ongoing communication that is unexpected but can be detected by your communication partner only.

Verbal masking techniques are part of SEEFs executive Social Engineering security awareness briefings.

9 About the Author

Dominique C. Brack is a recognized expert in information security, including identity theft, social media exposure, data breach, cyber security, human manipulation and online reputation management. He is a highly qualified, top-performing professional with outstanding experience and achievements within key IT security, risk and project management roles confirming expertise in delivering innovative, customer-responsive projects and services in highly sensitive environments on an international scale. Mr. Brack is accessible, real, professional, and provides topical, timely and cutting edge information. Dominique's direct and to-the-point tone of voice can be counted on to capture attention, and – most importantly - inspire and empower action.

Dominique Brack online:

- https://www.xing.com/profile/DominiqueCedric_Brack
- http://ch.linkedin.com/in/dominiquebrack
- http://www.slideshare.net/slideshare807am
- https://twitter.com/Reputelligence
- https://seef.reputelligence.com/

Icons Download:

- https://youtu.be/FPvgLUuDSYs - promo video
- http://selz.co/Ny-y91s5Z direkt link

Book QR code:

- Go there: http://bit.ly/1IYHDoN or https://reputelligence.selz.com
- Punch this in: 4ONLLC6X
- First name, last name and email is required [F0E0?] use a valid email and you will get the eBook sent to you.

