GUEST FEATURE

NLP-powered Social Engineering

by Anton Chuvakin & Gothstain <gothstain@meta-verso.com>

Mar 20 2001 4:34PM GMT

Abstract: This article deals with the problem of social engineering (SE) and how it can be powerfully enhanced by modern persuasion technology of Neuro-Linguistic Programming.

In the general discussion about the efficiency of information security defenses, such as whether a firewall can stop the specific attack or whether IDS of some kind will help, the important aspect is often being missed. Every computer system has a human using it, and that human is sometimes believed to be the weakest link in the information security chain. Since ancient times of legendary hackers, like Kevin Mitnick, the stories of Social Engineering (SE) attacks have been surfacing in the media. The attacks range from somebody emailing an AOL user with the request to submit their username and password that were supposedly lost during the computer upgrade to some hacker getting the chip layout of the new cellular phone via a simple call to R&D department.

The usual measures employed to protect from such attacks are often grouped together under "user education" and sometimes boil down to the pathetic "don't give your password to anybody" memo sent once a year to all employees. Unlike the technical countermeasures, the protection from SE is currently not well developed. But maybe there is nothing to worry about? While almost anybody can be taught to write some simple C in order to program exploits or simply operate somebody else's automated attack tool, it is believed that one should be born with exceptionally good "people skills" in order to perform high-level SE attacks. Well, this does not appear to be true anymore.

Lets jump back to 1975 when linguistics professor John Grinder and graduate student Richard Bandler started the new branch of psychology called Neuro- Linguistic Programming (NLP). And in 25 years that passed since, this new discipline has developed from modeling successful psychotherapists to full-scale description of human subjective experience, used in business, education, sports, sales and many other areas to achieve excellence. Why should computer security analysts concern themselves with somebody's "subjective experience"? The issue here is that NLP (where Programming is related to uncovering the programs that exist in humans, not really Programming their behavior - as some might want to see it) creates a powerful framework for persuasion and influence that expands well beyond psychotherapy. Now, as you are reading these lines, you might start wondering how this applies to SE attacks. And the more you think of it, the more you would be surprised by the answer. We all know that some people appear more trustworthy than others. Naturally we like some people more than others and are more likely to do what they want. And what they say seem to somehow make more sense. Is it some kind of "chemistry" of "charisma"? How surprised you will be to know that these things can be turned on at will? And, additionally, after changing what you say to people and how you say it just a little, your communication will powerfully increase its efficiency!

NLP persuasion toolkit, as taught by famous NLP trainers such as Kenrick Cleveland (www.maxpersuasion.com), John LaValle (www.purenlp.com) and Richard Bandler himself, contains several groups of techniques to drastically improve the impact of human communication. It all starts from building rapport, the state where you feel strongly connected to another person, begin to like him and feel you have many natural similarities. Rapport is achieved by pacing and leading techniques that

involve matching both verbal (WHAT you say) and non-verbal (HOW you say that and WHAT you do) components. We will give more details on this primary NLP weapon below. Then, as another person starts to like you and feel that you have their best interests in mind wide array of NLP methods can be used.

According to Dr Cialdini, the leading expert on influence, to be liked one should appear similar. As you think of it now, you start to understand that our life experience confirms that "law of influence". To create rapport one can match another person's behavior, habits, gestures, body posture, voice tonality, tempo and volume, eye movements and also beliefs and mood - any or all of the above. Several books are written on this subject alone.

Now we will turn to the infamous embedded commands: method of marking some parts of what you say with different voice tone or volume in order to slip under another person's conscious "critical radar". Smells like a huge pile of bullshit? OK, here is a simple two minute experiment that will naturally convince you of the power of the embedded commands: when talking to a group of people say this innocent phrase while slightly altering the way you speak while pronouncing the marked words: "Now we only *SCRATCH* the surface of this problem and nobody *KNOWS* what results we can achieve" and then notice how many people touched their noses! No magic, huh? Embedded commands can be used to direct people's experiences in the direction useful for the attacker.

Then go patterns of persuasive languaging: that help you effectively sharpen the blade of your verbal communication . As you start to become aware of the impact that NLP-enhanced communication will bring, your curiosity of what else is possible with it naturally grows. And as it grows, you can allow yourself to follow these words and begin to think how hackers might utilize the strategies and tools of NLP to get inside information about your network. And after you finish reading this article, you awareness of these new methods of social engineering will drastically expand. The patterns create the natural flow of language, help avoid objections and lead the listener to the desired outcome.

These and other general purpose tools are customized for each "victim" using the criteria elicitation and meta-programs. Just STOP now, and ask yourself: what motivates you more to do an unpleasant task: fear of your boss or the idea of having it out of your way so that you can do something more exciting? Lets suppose its the fear of the boss. OK, now if somebody calls and says "please reset my password to my login name or the BOSS WILL GET REALLY ANGRY!"? Doesn't it push you stronger into (maybe not the smartest) action than simple "please change my password" request? You just witnessed the "towards-away" meta-program play its evil role.

Meta-programs refer to those programs in our minds that control our behavior and describe another person's subjective reality. To understand Meta-programs you can think of "human software" that consist of thinking patterns, belief concepts, values, programs, etc. You can wonder right now how these programs can be recognized and elicited, but first you *must look* very carefully to the next analogy:

Computer Hardware = Neurology-Physiology
Operative System = Meta-Programs
Software = Thinking Patterns
Output Peripherals (monitor, printer) = Behavior (habits, language, etc)

Some meta-programs describe how people sort information in their minds. For example, if you take the Chunk Size/Reasoning Style meta-program, you can figure out what's the size of the "chunk" of information that people prefer to deal with when learning, communicating, thinking, etc. Some people go for details of things, they need to know everything in small chunks, so they see the trees, but not the forest. By contrast, some people sort information with the big picture, they want to see the general idea, so they can deduce small chunks from the big ones. They want the forest *first*, than the trees. NOW, you can understand why those meta-programs can be *very useful* in SE, because if you match a person's sorting patterns you'll be able to pace and then lead their behavior. Isn't it just great?

Another groups of tools, so-called "Sleight of mouth" (SOM) patterns are designed to reframe people's negative beliefs. *Negative* here refers to both negative to them and negative to the attacker (like, a belief that you should not email me the version of the firewall you are using is negative for the attacker and changing it might be desired). NLP assumes an ethical position with this powerful patterns, because they can be used to redirect people consciousness in seven directions so that

they are usually used for a win/win situation. The theory behind SOM patterns is that every external behavior stems from an internal state within a person. From that you can begin to reframe the way how your communication is accepted.

The following example elicits a positive intention (pace) and reframes an external behavior:

- [Joe]: Sorry, My boss isn't here, so I cannot give you any information...
- [gothstain]: Yeah, I understand your situation Joe. By the way, have you thought that your boss doesn't need to be there for you to give me the information? I mean, information is already there, and as you realize that your boss isn't always available to you, automatically you can save company time and money if you sent that information to me. Now, as you think about it, you can also realize how your efficiency can be rewarded later, because you saved company time and money.
- [Joe]: Hmmmm... Ok, can you repeat your e-mail please?

Time distortion is an another incredibly powerful tool: how happy would you be to buy our product the second time after you are completely satisfied with the deal you got the first time now? And as you look back from one year into the future when we already have the lasting business relationship, dind't it feel natural to sign the contract that made it possible? This tool is used to create a point of view from the future where your desired outcome is already a reality to the present where it was made possible.

As you probably realize by now, the tools (and we just barely scratched the surface of NLP persuasion methods) are really powerful and the one who knows how to use them powerfully can achieve outstanding results using for SE.

Another important application of NLP is customizing your own state of mind to create a solid foundation for SE. Are you curious now about what states am we refering to? If you are in a good state of mind, your language will flow easier, you'll gain rapport instantaneously, you will sound more convincing and you'll get the information you want faster. Attackers can also create states of mind in victims that feels so good that they want to be there for a long time thus creating a friendship that can later be utilized to elevate privileges or achieve some other goals attacker has.

However little can be done to protect the resources from advanced SE attacks (no firewalls, no effective intrusion detection, no patching for bugs) without going into compete paranoia rampage military-style some of the traditional infosecurity methods may still work. Penetration testing, for example can be very useful. One can hire an NLP-trained person and have him to perform penetration attempts by calling/meeting your staff. As usual, the amount of effort spent on such pen testing should be dependent upon the resources that are being protected. Then you can check if your company passes the test before a hacker does it in real life.

The solution that appear optimal to us (the cost of it can sometimes be prohibitive however) would be to "sensitize" your personnel to the typical SE attacks using NLP by making them aware of the "attack methods" that will be used. That will by no means make you 100% secure, but it is common knowledge in information security that nothing ever will...

Anton Chuvakin is a last-year graduate student at SUNY Stony Brook. Upon completing his PhD he intends to pursue a career in information security. NLP is one of his hobbies and he is certified by NLP Seminar Group International (Dr Bandler and John LaValle).

gothstain is a member of the Colombian research group InET (http://www.meta-verso.com). His hobbies vary from computer security to the deep understanding of the human mind.

Some resources on Social Engineering and NLP:

packetstorm.securify.com
http://packetstorm.securify.com/docs/social-engineering/

Psychology of Social Engineering
http://www.cybercrimes.net/Property/Hacking/Social%20Engineering/PsychSocEng/PsySocEng.html

Social Engineering Tips & FAQ

http://vampi.users1.50megs.com/social4.html

Mitnick: humans' the weakest link
http://www.securityfocus.com/templates/headline.html?id=8628

Information Security Reading Room - Social Engineering: A Backdoor to the Vault
http://www.sans.org/infosecFAQ/backdoor.htm

Wetware Hacking
http://www.artofhacking.com/Tucops/Etc/wetware/

NLP Information
http://www.purenlp.com/

NLP FAQ
http://www.purenlp.com/nlpfaqr.htm

Another NLP Resource Site
http://www.nlp.org/

NLP Training Site
http://www.nlpcomprehensive.com

Persuasion using NLP
http://www.maxpersuasion.com