Frogs in Hot Water

Amy Devine

11/4/2021

1 The Setup

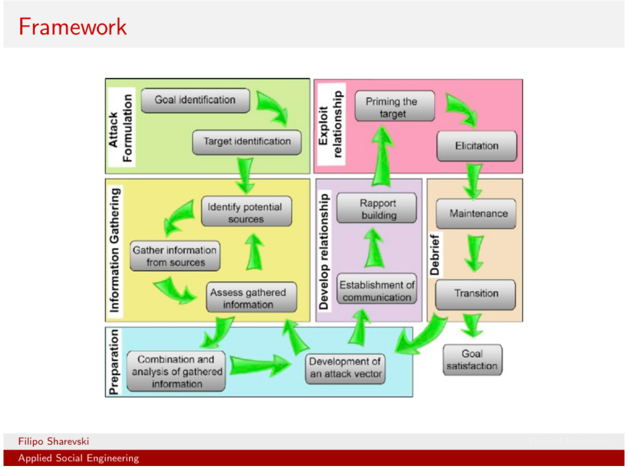
IBM has a nice and clean definition of automation

> Automation is a term for technology applications where human input is minimized.[3]

Social Engineering, though, seems to be human-centric where technology is a tool that is used by the engineer. Technology has improved the pace at which an attack can be developed, for example, by providing OSINT tools to search multiple databases that used to be done by hand. But still the human is in the drivers seat for an attack.

Figure 1 shows a workflow for a typical social engineering attack.[2] Each of the big-box steps can be accomplished through some level of automation given entrance and exit constraints.

It seems that the human is still very much a driver of the workflow; the human identifies the goal and performs the preparation step. For automation to be further incorporated into the attack workflow, an automation workflow would need to be able to further minimize the human input.



Framework

Filipo Sharevski
Applied Social Engineering

Figure 1: Social Engineering Attack Framework

For the purposes of this paper, let's assume that we have the mathematics and software frameworks to support the breakdown of the success criteria for each of the major and minor steps within the workflow. This doesn't seem too far of a stretch as it is just articulating a set of criteria that is typically performed by the human brain. How do you know if the information gathered from a source is credible or not? How do you know when the relationship between a con and a mark is developed enough to exploit? These are typically complex calculations that are performed by the human brain in seconds. Quantifying them would involve integration and quantification of various domains such as facial recognition, reputation of and trust in a source, tone or sentiment behind a piece of information. Currently, there is work underway to explore and quantify many of these domains. [4][5] NIST is already engaged in the area of biometric recognition meaning that this will become a regulated industry.[6] Fusion of all the available domains of information is surely not that far off.

Fusion, though, occurs in the digital domain - a medium that computers can understand and programs can follow their predefined if-else statements to their conclusions. As technology advances, it will be interesting to watch how the ”je ne sai quoi” of human comprehension and deduction is boiled down to a string of 1s and 0s. It would be an opportunity for self-education and reflection, for sure, and potentially the knowledge to then alter oneself to manipulate the feedback loops into the system.

2 Social Engineering Influence

Social Engineering is pure influence. Assuming that there is no limit to the computational power and speed of automation calculations, we can assume that alterations to the master plan can be made with the same speed as the human mind. When a system is developed possessing the mathematical ability to quantify the validity of information received purely from digital means, then reality becomes individualized. Again, not very far off as we have segmented markets of 1 and customization of almost everything in our lives today. Targeted ads served up based on previous shopping experience. Add in a faster, more robust sense of customization and we have reality shaping content served up.

What do The Truman Show and Wanda Vision have to teach us about individualized reality? These shows are about individuals that are living in carefully constructed worlds where (the real) reality finally breaks through. Somehow, the unconscious mind may realize that the reality isn't...well, real. Is this a failure in the algorithms? The Truman Show had a light fall down from the sky. Wanda Vision had reality also trying to break through the radio. Maybe a sign that we can choose to accept the reality bubble that has been created for us but that the outside world still keeps doing its thing.

3 Reflection

Automation tasks out the redundant processes humans engage in today. Today, automation processes appear limited to tasks that are well-defined with a predictable outcomes. For example, algorithms are trained against existing (mostly English) content to determine the intent (through style-based analysis) or accuracy (through knowledge-based analysis) of the content. This is a human process expedited through technology.

The only kick-start an autonomous social engineering system would need is definition of the initial goal much like the drop of an unsuspecting frog into the room temperature water. After that, the system can slowly increase the manipulation of reality continuously altered in a mass amount of consumed media. And with each nudge, each slight change, reality will adequately prime targets to the desired change. The autonomous system working in the background to adapt messaging based on feedback which is then pushed back out in content. In the end, we are like the frog. Cooked.

References

[1] Xinyi Zhou and Reza Zafarani. 2020. A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities. ACM Comput. Surv. 53, 5, Article 109 (September 2020), 40 pages. https://doi.org/10.1145/3395046

[2] CSEC 597 - Week 4: Applied Social Engineering, Traditional Social Engineering Attacks

[3] https://www.ibm.com/topics/automation

[4] https://defensesystems.com/articles/2020/08/11/facial-recognition-trust-autonomous-systems.aspx

[5] Safra, L., Chevallier, C., Grèzes, J. et al. Tracking historical changes in trustworthiness using machine learning analyses of facial cues in paintings. Nat Commun 11, 4728 (2020). https://doi.org/10.1038/s41467-020-18566-7

[6] https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0

[7] https://www.chicagotribune.com/news/ct-xpm-1998-07-05-9807050337-story.html