Strength and Weakness of Information Security: Human Nature

Phuong T. Tran
Department of Computer Science
Columbus State University
Columbus, GA USA
tran_phuong@colstate.edu

Abstract—In today’s society, information has become so readily and instantly available that the search engine, Google, has been incorporated into the English vernacular. With this explosive growth of information availability, however, comes increasing concern for security. Today’s information security systems are designed to be highly secure, yet information is leaked anyway, and many of these security failures lie in the human factor—in both creativity and negligence. In “The Psychology of Security,” West discusses the psychology of human risk assessment and why end users make bad security decisions. Humans will always be the weakest link in any information security system because we can create these systems, we can exploit any flaws in the creation of it, and we are imperfect and can be negligent. However, a study of psychology is not enough, at least not individual psychology as described by West. Humans are complex as individuals, but they become a different entity as a group. To study and model whole environments is necessary, as well as using both individual and organizational psychology and also quantitative system dynamics to help create security and privacy policies that adapt to dynamic environments and work with the security technologies today. Adaptability is the key because ultimately, no matter how tightly written and implemented security policies and features are, breaches due to human creativity or negligence can only be mitigated.

I. INTRODUCTION

A discussion of information security would aptly be prefaced by Auguste Kerckhoff’s principles that define a secure cryptosystem. In his treatise on military cryptographic, La cryptographie militaire, Kerckhoff delineated the following requirements for a secure cryptosystem:

1. The system must be practically, if not mathematically, indecipherable;
2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
4. It must be applicable to telegraphic correspondence;
5. It must be portable, and its usage and function must not require the concourse of several people;
6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe [1].

The one-time pad cipher fulfills all of these criteria and therefore is a provably secure system. With current mathematical technology, the cipher cannot be practically or mathematically deciphered, nor does the method of creating a one-time pad need to be kept secret. The key would be changed each time, so there is no need to retain it—only a need to destroy it and not reuse it, and the cipher can be generated by hand, having been a system created before the advent of ubiquitous computer use [2].

As secure as the one-time pad cipher is, it is only as good as the people who create the pads. The one-time pad cipher was used to much success during the 1940’s for military use. However, in the case of the VENONA ciphers, human flaw in generating the pads caused some pads to be used more than once or “in depth” and thereby resulted in the deciphering of the messages by unintended parties. Recall that the one-time pad cipher’s requirement to remain secure is that the key not be reused. The VENONA ciphers incident, quite aptly shows how a secure system can be compromised through misuse. In addition, the disclaimer that is always said when citing that the one-time cipher or any cipher is secure is that as of yet, the mathematical problem of solving the cipher is difficult and impractical. No one knows if it is impossible, and with human creativity, it may be possible one day, as going to the moon has been possible for our civilization [2].

Any security system then, whether it may be a simple lock and key measure or a complex cryptosystem to encrypt a message, has as one of its flaws, the human factor because we imperfect humans are the ones who created that system. This logical, but oft forgotten statement is the cause of many security system failures. Human beings are flawed by nature and the work produced and the usage of the system would thereby be flawed. Even if theoretically perfect, the power of human creativity would be able to “break” what it has created—that is, humans created the lock and key, and they also created the lock pick.

The human factor can puncture the tight wall of a security system in generally three areas: 1) the faulty creation of the system, e.g. a software bug leading to failure; 2) malicious exploitation of an otherwise innocuous bug; or 3) incorrect, ignorant, or negligent use of an otherwise “secure”
In “The Psychology of Security” West proposes a method rooted not in hard scientific technology, but rather in psychology, specifically in how humans assess risk and react to it. He proposes that in system administration and software usage, administrators and developers need to consider at every stage, ways to better notify users of risk and to help users better understand those risk in order for them to make the correct decision. Moreover, the system needs to also reward the user or provide some tangible feedback that the system is working and that the decisions they make do matter [3].

West lists several reasons why security fails at the user level and why the user makes bad decisions when given a security choice, e.g. going to a web site whose certificate has expired. These reasons are summarized below:

1. Users do not recognize that they are at risk.
2. Users are not motivated.
3. Safety and security are abstract concepts that have no clear reward or punishment.
4. Users tend to gamble when it comes to risk assessment if their loss is not a guaranteed one.

As humans, users tend to think that bad things do not happen to them or that they are safer than other users. On the other hand some users who do implement security features, such as firewalls, may engage in more risky behavior, such as a driver might because he/she is wearing a seatbelt. The article also notes that users tend to follow the status quo and usual actions instead of reading all screen notification messages. That is, users may just automatically click “OK” through all dialog boxes to get on with their work. Moreover, safety and security are quite abstract to most users. Humans need a clear reward or positive reinforcement system. Having something bad not happening is not sufficient to a user since no reward is perceived. Nor does negative reinforcement come immediately, and by then the user does not associate the bad action with the negative reinforcement. Therefore, the user resumes the “unmotivated” mode [3].

Lastly, users tend to gamble when it comes to risk assessment. West addresses the following scenario:

1. Guaranteed $5 loss
2. Possible $10 loss or a chance of no loss at all.

West says that most users will choose the latter scenario. In a real world computing situation, this would equate to a user going to a site where the certificate has expired. If the user does not click through, then the user gets nothing. If he/she does, then he/she may get to the website and with no further consequence. Many trusted sites have no consequences for clicking through them when the certificate is expired. When no negative reinforcement is present, the user then stores that under his/her list of routine and “unmotivated” status quo things to do and makes the choice more likely in the future, potentially for a more malicious site [3].

To combat this, West proposes further research into human risk assessment. He also suggests that warnings and awareness be more available and more discernible than other, more routine messages. In addition, a reward, even something in the form of a dialog box notifying the user of the result of the user's action. West says that negative reinforcement should not be ignored either and that employees need to know and be shown the consequences of making bad decisions. Finally, since humans tend to be creature of habits, many are happy with decisions being made for them. Overhead costs could be reduced simply be creating a set of defaults. However, since no one can account for all circumstances, the aforementioned methods need to be implemented too [3].

The downside to West's proposals is inherent in the human behavior that he bases his solutions on. Though both positive and negative reinforcement is always important, an inundation of messages would desensitize the user to the messages. Users would then relegate themselves to the unmotivated pattern that West described. Secondly, though most users are creature of habits, one cannot deny the curious and creative user who will ask why and try to get around defaults. Despite these shortcomings, West's approach to using psychology is a very viable component of a solution to better mitigate the human factor in information security.

The next section will discuss extensions of West's proposal into a system of users and a more quantifiable model for system dynamics, followed by a proposed solution that will look at how individual and organizational psychology can be translated into users and systems in an information security world.

II. RELATED WORK

Trcek in “Security Models: Refocusing on the Human Factor,” takes an abstract look at users as a system and applying principles of system dynamics and agent technologies to create a more quantifiable model of human interaction, especially in regards to risk assessment and management. The system dynamics model that Trcek uses looks at causes of increased risk as well as any feedback loops to discover relationships and how to decrease risk. System dynamics modeling looks at a broader view beyond the individual user. This would be useful for modeling larger businesses, such as those with multiple facilities, and is important because each entity has a different “personality” than the individual [4].

In addition, Trcek also proposes the use of agent technologies which model “agents” and their interaction with the environment to generate patterns of behavior. Agent technologies, then would be the abstraction of the human user (though not necessarily so; agent technologies could also represent technological components) that West discussed from a psychological point of view. The advantage of agent
technologies would be the ability to study patterns of behavior without the expensive process of recruiting users for experiments. The disadvantage of course is that no model can be a true substitute for humans.

In “Security and Privacy Challenges in Open and Dynamic Environments,” Kagal et al. gives a more real world look at a system that Trcek might model and one that West might analyze on a psychological level by studying the case example of a hospital system as an open and dynamic environment where privacy is of the utmost importance. In a hospital system, users are typically “floating,” and they may have different roles from one day to the next. In such a mercurial system, standard role-based authorizations are tedious at best. Instead, Kagal et al. proposes a system that derives from the “real world” ideas of a shared vocabulary or language to define specific, adaptable policies and also an authorization system based on a user’s attributes and “trust.” [5] The promising part of Kagal et al.’s model is that it takes into account new users into the system or even floating users, as in the hospital system example. The disadvantage of Kagal et al.’s system as currently described, is that as is with humans and trust, the flexibility of the system leaves it open to “lies.”

III. FUTURE RESEARCH
The papers by West, Trcek and Kagal et al., all provide great models for further understanding the human factor in information security, and they also propose tools for mitigating the effect of human creativity and negligence. Kagal et al.’s model is the most promising, but it would benefit from the analytical tools proposed by West and Trcek. The development of a “language” with which to construct specific policies that is both easily understood by the user and implementable by a computing technology is essential. The definition of trust is also an integral part of Kagal et al.’s model. However, the societal norms and trust that Kagal et al. based their model on are norms that are quickly changing in a world where society is truly global in communication and where a “friend” is only a click away on Facebook.

Current studies of psychology and computing technologies do not provide enough information as to what is needed for reinforcement or motivation for an office worker who is at the computer for more than eight hours a day. Reactions that individuals now have in an increasingly digital society are very different than what they were even five years ago. The “system” that a user belongs to can now span the entire world. The first study that would need to be done is to expand upon Trecek’s idea of agent technologies by standardizing a life simulation where behaviors can be studied and patterns quantified. From fantasy worlds to real-life simulations (such as secondlife.com), millions of people are already engaging in such simulations where they take risks, cooperate with other users, and develop trust in an open and dynamic, but “safe” and entertaining environment. Simulations allow for greater control and standardization for studies and also to test models than other experiments. Education of a user can also occur through interactive simulations that show users where they can effect change and feel a part of the process. From these studies of behavior and pattern, reinforcements and motivators can be derived and tested. In human development, behavior comes first and then language and rules, and so it should be to develop a system similar to Kagal et al.’s. With that knowledge and understanding of the end user, a system can be built that the user understands and is invested in, and that will be a system that the user will more likely protect.

IV. CONCLUSION
The human factor and the flaws that it produces are something that cannot be controlled, but only mitigated through awareness and reward. Humans will always be the weakest link in any system, not because of any lack of ability, but because of that almost fathomless creativity and free will. Yet, humans are also the strongest link in having created the system in the first place. On the flip side of psychology are models for system dynamics that map usage information into more mathematical simulations, as described by Trcek. Kagal, et al. discusses the application of security and privacy policies in the dynamic environment that Trecek seeks to model. Using present-day tools of simulations, psychology of users in a digital world can be analyzed and quantified, and then that data can be used to create the “policy language” and authorization model for increasingly open and dynamic systems. Combined, the proposals of West, Trcek and Kagal, et al. are what is needed to engineer the security systems of the future. In essence, the key to engineering a good security system is to understand the user, and information security will become an interdisciplinary field spanning computer science to system dynamics to game theory and to psychology.

REFERENCES