Keep your attackers close but your users closer

Lauren S. Ferro
lsferro@diag.uniroma1.it
Sapeinza University of Rome
Rome, Italy

ABSTRACT

STRIDE is a model used to help classify threats, which relies on identifying attacker related threats rather than those caused by human errors or related factors (e.g. Stress or Lack of Knowledge). Therefore, users (and their behaviour) become an attack vector for various types of attacks and exploits to target. As a result, it can leave a well calibrated and designed system and its data vulnerable due to human error. Therefore, this paper proposes a preliminary variation of the STRIDE model - *STRIDE-HF* that proposes the consideration of human factors as part of STRIDE.

CCS CONCEPTS

• **Security and privacy → Systems security**; **Human and societal aspects of security and privacy**; • **Human-centered computing**;

KEYWORDS

human factors, cybersecurity

1 INTRODUCTION

Many models of threats exist, which aim to understand the type threats that exist within cybersecurity. One key model is STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). This model, developed by Garg and Kohnfelder [2], helps to classify threats (along with its variations such as STRIDE-per-element and STRIDE-per-interaction). However, STRIDE focuses on threats in the context of hackers or exploits, and it, like many other similar models or techniques (e.g. Attack Trees and Attack Libraries), overlook the foundational issue of user behaviour, which in most causes, is the cause of allowing attacks to occur.

1.1 Human Factors in Cybersecurity

To understand what is likely to influence an attacks success, we need to focus on the vulnerabilities of human behaviour. Therefore, by centering approaches for security on areas where users are more likely to make errors, we can consider the human factor as part of the STRIDE model. Human factors, also known as the *"Dirty Dozen"* [1] is a twelve item list, consisting of: *Lack of Communication, Complacency, Lack of Knowledge, Distraction, Lack of Teamwork, Fatigue, Lack of Resources, Pressure, Lack of Assertiveness, Stress, Lack of Awareness,* and *Norms.* While the initial context of Human factors was in aviation maintenance, within the context of cybersecurity, we can identify situations where any of these Human Factors are or can be problematic. For example, in high stressful jobs, *Stress*, *Pressure*, and *Fatigue* are likely to have an impact on users decision making processes where trade-offs are made when important steps in a process are missed in favour of efficiency.

1.2 STRIDE-HF

STRIDE-HF (human factors) preliminary consists of Human Factor issues that theoretically correlates with the STRIDE categorisation. The difference with STRIDE-HF, is that rather than focusing on solving the problem against the *attacker*, it focuses on the weaknesses and vulnerabilities of the *user*. For example, traditionally, resolving an issue centred on *Spoofing* would likely focus on finding ways to prevent unwanted access (e.g. locking accounts). The same example in the context of STRIDE-HF would focus on factors such as *Stress* or *Lack of Awareness* as being the attack vectors and to develop a threat model and/or solutions to address these (e.g. enforce breaks during long work days, provide support during stressful work periods, etc.). In this way, reducing the likelihood of a well designed system being let down by the users who are stressed or unaware of the risks involved in performing various actions (e.g. not scanning downloaded files). The development of STRIDE-HF requires first that STRIDE related issues are examined through the lens of Human Factors, where we can begin to anticipate which Human Factors are more likely to align with the STRIDE categories and more importantly how. Ideally, the STRIDE-HF model will begin with analysis of several Human Factors and STRIDE categories and conclude with an examination of all STRIDE categories and Human Factors. As a result, one can make recommendations about ways to deal with relevant Human Factors and STRIDE categories within the workspace that may compromise the security and integrity of the system and its data.

1.3 Conclusion

Research within this area also presents an excellent opportunity to contribute to the field of threat modelling, as suggested by [2] that ideally focuses on the ideology where "prevention is better than a cure". To this end, if we can reduce even the likelihood of human error, via a model that considers humans - *especially Human Factors* as part of the development of threat models, we have the potential to better improve the security of systems and their data. As a result, we anticipate that this model is iterated, refined, empirically tested, and applied to different areas of cybersecurity.

2 CITATIONS AND BIBLIOGRAPHIES

REFERENCES

[1] Gordon Dupont. 1997. The dirty dozen errors in maintenance. In *The 11th Symposium on Human Factors in Maintenance and Inspection: Human Error in Aviation Maintenance.*

[2] Adam Shostack. 2014. *Threat Modeling: Designing for Security.* John Wiley Sons. Google-Books-ID: YiHcAgAAQBAJ.

womENcourage '19, September 16–18, 2019, Rome, Italy
2019. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn