Combining threat models with security economics

Per Håkon Meland*

Norwegian University of Science and Technology, per.hakon.meland@ntnu.no

Abstract

In order to defend against cybersecurity threats, we need invest in appropriate protective and reactive security measures, however, we also have to accept that *perfect* security will never be a reality in practice. The adversaries have a huge economic advantage and defenders cannot uphold a sustainable security budget in the long run.[1]

Threat modelling typically involves techniques where someone, e.g. a security expert or system owner, tries to think like an attacker in order to determine how systems can be attacked and exploited. In many disciplines, threats are estimated based on stochastic models developed from historical data, e.g. the expected next time to failure for a hardware device or extreme weather frequencies. However, cyberattacks is a relatively new phenomenon, and the attackers are strategic adversaries and not comparable to random natural events. The general unavailability and unreliability of historical data makes it difficult to estimate the likelihood of attacks, especially in areas with rapid technological advances. Therefore, we commonly start from assumptions about the adversary's capabilities, but just as important, we need to consider the financial motivations of possible adversaries.[2] This perspective is regarded as essential for understanding the state of cybersecurity today, as well as how to improve it moving forward.[3]

The goal with this study is to answer the following research question: *How can threat models in combination with economic incentives improve cyber risk quantifications?* When developing these models, there is a need to accept the general unavailability of reliable historical data, and instead build on data about the present to project the future. Identifying reliable data sources and models for opportunity cost for attackers and losses for defenders will be of benefit when estimating likelihood and severity for unwanted events. For example, it is possible to study the mechanisms and trends of the cybercrime market in order to improve our situational awareness about threats in the environment of our system.[4] Market prices contain some information about expectations and may serve as forward-looking indicators, in contrast to statistics calculated from historical data.[5] This is comparable to the arms market in the real world; if there is a high demand for aggressive weapons, then someone might be planning an attack. Also, if you are able to identify that the buyer of these goods happens to be a group or country with a grudge against you, then it is wise to install defence mechanisms that can handle the type of weapons that have been sold. In the cyber world, these dynamics works at a much higher speed, giving the defenders a preparation time of maybe hours or days.

*The author presented the paper at the NISK 2018 conference.

[1] Ross Anderson. "Why information security is hard-an economic perspective". In: *Computer security applications conference, ACSAC 2001.* IEEE. 2001, pp. 358–365.

[2] Tyler Moore and Ross Anderson. "Economics and Internet Security: A Survey of Recent Analytical, Empirical, and Behavioral Research". In: (2011).

[3] Tyler Moore. "The economics of cybersecurity: Principles and policy options". In: *International Journal of Critical Infrastructure Protection* 3.3-4 (2010), pp. 103–117.

[4] Shari Lawrence Pfleeger and Deanna D Caputo. "Leveraging behavioral science to mitigate cyber security risk". In: *Computers & security* 31.4 (2012), pp. 597–611.

[5] Ross Anderson et al. "Security economics and the internal market". In: *Study commissioned by ENISA* (2008).

Proceedings of the 11th Norwegian Information Security Conference, Sep. 19-20, 2018.
NISK Journal, e-ISSN 1894-7735. https://ojs.bibsys.no/index.php/NISK