Cyber security exercises as a platform for cyber security experiments

Teodor Sommestad, Jonas Hallberg
Swedish Defence Research Agency, Linköping, Sweden

***Abstract*—Reliable empirical data is difficult to obtain in the cyber security field. Security theories, frameworks, methods and measures are therefore rarely validated empirically. This paper proposes the approach to collect empirical data in conjunction with security exercises. Several types of experiments can be performed during a security exercise, at a small cost.**

I. Introduction And Background

Cyber security is an important topic and a lively research area. A plethora of frameworks, methods, tools and principles can be found in literature. However, few of these have been validated empirically. For instance, Verenedel's [1] review of proposed security metrics illustrates the lack of empirical basis for the underlying theories. Of the 90 papers reviewed, a minority attempted to empirically validate the metric or measurement method proposed, and these tests often comprise of a comparison to domain experts beliefs.

There are a several reasons for the lack of empirical data in the field. Data related to security (e.g. incidents, security measures) are sensitive and often treated as confidential [2]. Even if the actual incident data from a representative sample of organizations would become available to the public (or just researchers) it would be difficult to draw general conclusions from this data due to the risk of various types of bias. E.g., if organizations would report the incidents they have experienced during a year this would only cover the incidents they actually observed and documented. But many incidents are difficult to observe even after they have occurred. Hence, it is difficult to obtain reliable security related data from operational systems.

Experimental studies that explore the strength of security measures typically explore the capabilities or limitations of some security technology. While such studies make important contributions, it is difficult to generalize the results to an operational context. These experiments test a well-defined set of attacks; however, it is difficult to know which of these attacks an operational system will be exposed to.

Metrics such as the expected probability of success for attackers [3] and the adversary work factor [4] are practical from a decision makers standpoint. These metrics communicate the security of a system by stating something about the attack that is required to compromise the system. A metric of this type offer valuable input to a risk management process and do not require that decision makers know or hypothesize about what attacks the system will be exposed to. To conduct experiments with such variables as the dependent variable is not a new idea; however, the cost associated with experiments has meant that only a handful has been performed. This paper suggests experiments in conjunction with security exercises (i.e. where security experts are trained) to investigate what attackers' success depend on.

II. Results

The Swedish Defence Research Agency has created the National Centre for Security in Control Systems for Critical Infrastructures. Security exercises have already been performed in this centre's computer cluster and valuable empirical data has been obtained from the international exercise called "Baltic Cyber Shield". Our analysis of the experimental properties of security exercises shows promising results. A security exercise offers the possibility to control and measure variables just as in an experiment, but at a shared cost between the experiment and the exercise.

Controllable variables in security exercises include: the configuration of the targeted system, the security measures installed, the vulnerabilities present, the attack target, the tools used by the attackers, the information about the target available to the attackers, the skill of the attackers, and the time attackers have available. Several variables can be measured in addition to the controllable variables, including: the time attackers spend on different stages and goals, the attempts they make, the success they have, and the prioritizations they make.

Hence, experiments conducted in relation to security exercise are at a comparably small cost and have the potential to produce meaningful data. First and foremost, they can be used to test the impact that different protective measures have on the effort required by attackers or their success rate, in a realistic context. These measurements can be used to test the validity of common security theories and the accuracy of common metrication methods. By controlling the attackers involved the data can be used to assess properties associated with skilled and unskilled attackers. Furthermore, the accuracy of forensic methods can be assessed by testing their ability to recreate logged attack scenarios.

References

[1] V. Verendel, "Quantified security is a weak hypothesis: a critical survey of results and assumptions," *New Security Paradigms Workshop*, 2009.

[2] D. Geer Jr, K. S. Hoo, and A. Jaquith, "Information security: why the future belongs to the quants," *Security & Privacy, IEEE*, vol. 1, no. 4, pp. 24–32, 2003.

[3] L. A. Gordon and M. P. Loeb, *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, vol. The Mcgraw. New York, NY, USA: Mcgraw-Hill, 2006.

[4] G. Schudel and B. Wood, "Adversary work factor as a metric for information assurance," in *Proceedings of the 2000 workshop on New security paradigms*, 2001, pp. 23–30.