Tool, Technique, and Tao in Computer Security Education

Zhenkai Liang
National University of Singapore
liangzk@comp.nus.edu.sg

Jian Mao
Beihang University
maojian@buaa.edu.cn

Abstract - Computer security is a broad subject, covering topics in many subject areas of computer science. Moreover, this large body of knowledge is also actively changing with rapid advancement of computing technologies. In computer security education, students need the right methodology; otherwise they may feel at lost when facing the fast-changing security landscape. In this article, we discuss the approach and experience we had through several years of practice in computer security education. We advocate focusing on the fundamental concepts, to achieve deep understanding and flexible application of security knowledge through repeated reflection.

Keywords - Computer security education, Methodology

I. Educational Objectives

Educational objectives can be classified into several tiers [1]. Based on this taxonomy, Anderson et al. [2] revises the taxonomy of learning, teaching, and assessing as: *Remember*, *Understand*, *Apply*, *Analyze*, *Evaluate*, and *Create*. It is also a measure of how deep students understand knowledge: they may remember and understand *what* is the knowledge; they may learn *how* the knowledge can be applied to solve new problems; ultimately, they may know *why* the knowledge is created, and thus can analyze and evaluate existing knowledge and create new one. In the Chinese traditional philosophy, the levels of understanding (*what*, *how*, and *why*) are formulated as three corresponding levels of proficiency:

- **Tool (器):** Simple usage of basis of knowledge**.**
- **Technique (术):** Flexible application of knowledge.
- **Tao (道):** Fundamental understanding beyond the subject area.

Each individual has his/her unique view of the world and own way to learn new knowledge. Learning is a process to digest knowledge and transform it into an internal representation specific to each individual. Therefore, the only way to achieve understanding at the deepest level is through self-reflection, connecting and "compiling" knowledge into the inner representation of each individual.

II. Methodology for Learning in Computer Security

Education of computer security has been actively studied. Many efforts have focused on the curriculum and overall strategy in computer security education, such as the work by Bishop [3] and Moses-Petullo [4]. In addition to theory and abstract knowledge, hands-on practice is a critical aspect of computer security. To this end, Vigna [5] describes experiences in hands-on education of network security using live exercises on a testbed. Du et al. [6] developed a series of experiments for computer security education. They have demonstrated that such hands-on experiments play a key role in deepening students' understanding.

However, computer security is a fast changing field. Knowledge and tools are often outdated soon after, if not before, they are taught. It is difficult for curriculum and experiments to keep up with the rapid changes. To counter this challenge, we need to guide students to understand beyond the subject knowledge itself, to reach the reason why it is developed, and its connection with other knowledge.

Inspired by the principles of Chinese martial arts, whose ultimate goal is to build up the internal of a person's mind rather than to train the skills for physical movements, we believe the following principles from Chinese martial arts are inspiring to computer security education:

- **Countering changes with a constant principle (以不变应万变).**
- **Counter force with flexibility (以柔克刚).**

A constant principle leads to deep understanding of computer security knowledge, which will embed students with a set of methods to approach a large range of security problems. It also allows students to connect the knowledge well, so that they are flexible and quick in finding solutions.

What is the constant principle that enables flexible applications in computer security? We view computer security as *a new way of thinking*. For a new topic/area, the students should first focus on understanding how the system works. However, in addition to merely understanding it, they should think in a different angle as an attacker, to see how the system can be compromised, namely *break the system*. Next, it comes to understand the attack for how/why it works. The students can then think as a defender and see how to break the attacks to strengthen the system, namely *break the attack*. This will complete a cycle to bring the system with enhanced security, which also starts off another cycle of "Understanding (System) - Breaking (System) - Understanding (Attack) - Breaking (Attack)." This learning cycle is summarized in Figure 1.

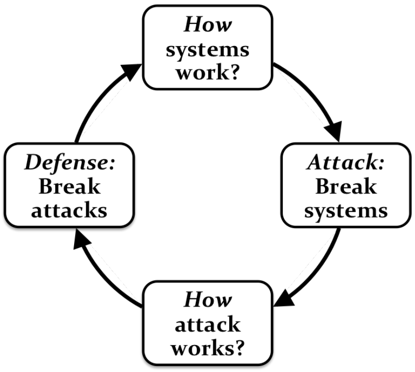

Figure 1. The learning cycle of computer security.

To equip students with this methodology, we need to guide them to practice; and more importantly, to reflect. In our teaching practice, we show how the cycle happens in many subjects. Taking the buffer overflow attack as an example, we start off by introducing the Intel architecture and illustrating how function call works. Then it is natural for students to "see" the buffer overflow attack by themselves. By analyzing the requirements of buffer overflow attacks, we show how defense solutions, such as stack protector and address space layout randomization (ASLR), break certain requirements of the attack. This process is illustrated in Figure 2.

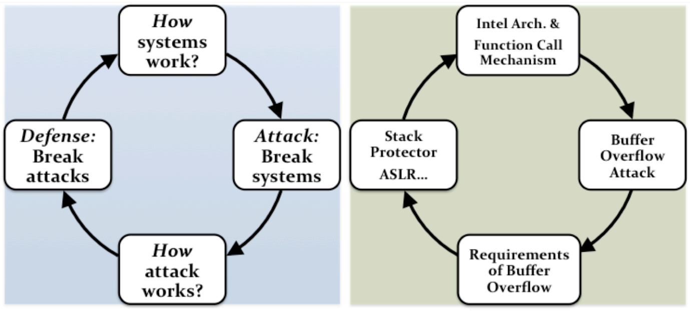

Figure 2. Mapping the learning cycle to buffer overflow attacks.

To help students reflect and grasp this methodology, we repeatedly show how to abstract this cycle from many topics in computer security, e.g., software security, web application security, and network security. In this process, they get the opportunity to strengthen their own understanding through the repeated exposures to this learning cycle in the context of many subjects.

III. Mission of University Education

In today's information age, many resources and services are readily available for training people, for example, the MOOC (Massively Open Online Courses). The strength of such resources and services is in *delivery* of knowledge, which is more about the tool and technique aspects of understanding. However, deep understanding at the Tao level needs individual reflection. So in our opinion, one of the unique strengths of university education is in individually guiding students to reflect, so that they can gain true understanding, enabling them to explore and innovate.

Concluding, we believed that one of the key missions of a quality university education is to engage students in actively thinking and reflecting. It can be summarized by the following Chinese proverb: 静思悟道 (Quietly thinking to reflect on Tao)

- **Quietly Thinking (静思):** The amount of information available to today's students is a blessing as well as a distraction. We need to teach students how to discard irrelevant or unimportant details so that one can focus on the principle.
- **Reflecting on Tao (悟道):** We should guide students on how to digest knowledge into their inner representation, achieving understanding at the deepest level.

Acknowledgments

We thank the editors for their comments to improve this paper. We thank Soo Yuen Jien, Ben Leong, Damith Rajapakse, and other colleagues for their inspiration and valuable comments.

References

[1] Benjamin S. Bloom. *Taxonomy of Educational Objectives: Handbook I: Cognitive Domain*. New York: David McKay, 1956.

[2] Lorin W. Anderson and David Krathwohl. *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives.* New York: Addison Wesley Longman, 2001.

[3] Matt Bishop. *Teaching Computer Security.* In Proceedings of the Eighth International Conference on Information Security, 1993.

[4] Kyle V. Moses and W. Michael Petullo. *Teaching Computer Security.* In Proceedings of the ASEE Middle Atlantic Section Meeting, 2014.

[5] Giovanni Vigna. *Teaching Hands-on Network Security: Testbeds and Live Exercises.* In Journal of Information Warfare, vol. 2, issue 3, pp 8-24, 2003.

[6] Wenliang Du, Karthick Jayaraman, and Noreen B. Gaubatz. *Enhancing Security Education with Hands-on Laboratory Exercises.* In Proceedings of the 5th Annual Symposium on Information Assurance (ASIA '10), 2010.

Zhenkai Liang is an associate professor at School of Computing of National University of Singapore. His main research interests are in system and software security, web security, mobile security, and program analysis. As a co-author, he won six best paper awards. He also won the Annual Teaching Excellence Award of NUS in 2014 and 2015. He received his Ph.D. degree from Stony Brook University, and B.S. degree from Peking University.

Jian Mao is an assistant professor at the School of Electronic and Information Engineering of Beihang University. Her main research interests include cloud security, web security, and mobile security. She won the First-class Teaching Award from Beihang University in 2012 and 2014. She received her Ph.D. degree and B.S. degree from Xidian University, China.