The Strengths and Challenges of Analogical Approaches to Computer Security Education

Matt Bishop[1] and Kara Nance[2]

[1] University of California Davis, Davis, CA USA
bishop@cs.ucdavis.edu
[2]University of Alaska Fairbanks, Fairbanks, AK USA
klnance@alaska.edu

Abstract. When teaching concepts such as computer security, with which students cannot easily identify, it is frequently helpful to use analogies to attempt to map a complex concept to an idea with which the student can identify. While this method works particularly well in the computer security domain, there are associated challenges and limits that must be considered when creating appropriate analogies. This paper defines analogies, provides some specific examples in the computer security realm, and discusses the challenges and limits associated with this approach.

Keywords: Computer Education, Computer Security Education, Analogies

1 Introduction

Computer security is a complex subject, one requiring both an understanding of broad concepts and an attention to fine detail. Students of computer science understand this, because much of systems work in computer science has the same properties. One must understand the concepts, and then design and implement systems with great attention to detail; to be sure they perform at the requisite level. But this complexity can be very difficult to convey to non-computer scientists and new computer scientists.

Even more difficult to convey are certain basic ideas that, while clear to practitioners, are counter-intuitive to most people. As an example, consider the definition of "security" itself. The dictionary definition is "the state of being free from danger or threat"[1]. Some people feel secure in their homes, because their sanctuary has never been invaded by malicious people. Others feel differently, especially victims of home invasion crimes. Some people feel secure giving merchant web sites their credit card information, to make shopping easier (and to avoid re-entering the credit card information each time); others want the security of not leaving that sensitive data in the hands of another. In life, security is largely a matter of perception, culture, environment, individual desire, and can vary from moment to moment. Thus, the notion of security varies among people, and varies in ways that people seldom investigate, realize, or appreciate.

This paper discusses an approach to conveying computer security concepts to non-technical audiences through the use of analogies. We provide some background in the next section, and then present some example analogies. A discussion of the challenges associated with finding good analogies, and teaching students how far analogies can be taken, make up the fourth section. We conclude by suggesting other techniques based on analogies that may prove useful.

2 Background

Educators, political organizers, marketing personnel, and parents are well aware of the importance of communicating in the language of the audience. Saul Alinsky wrote, "People only understand things in terms of their experience, which means you must get within their experience" [2, p. 81]. As an example, consider the number of stars in the universe. Presenting the concept mathematically by telling an audience there are 9,000,000,000,000,000,000,000,000 stars in the observable universe conveys little meaningful information about the magnitude of the number of stars, because most people cannot think of anything within their own experience to associate that number with. Alternatively, when the audience hears there are more stars in the observable universe than there are grains of sand on all the beaches of the world, their eyes light up. They have been to a beach, and probably to many beaches. They know how much sand is on those beaches. Now, they have a better understanding of the number of stars in the universe because the concept has been mapped to something with which they can identify.

This is particularly important when students are thrust into environments with which they are unfamiliar—such as using a computer. In order to bridge the distance between the instructor and the student, the instructor needs to find a way to help the students to identify with the concept. An identification of common ground between the instructor and student can be used to introduce a seemingly unrelated concept that is easy for the student to understand or identify with. This idea can then be transformed or bridged into the specialized realm that the instructor is teaching to share the idea with the students. An effective tool for accomplishing this bridging activity is an analogy.

3 Analogies

An analogy presents a concept or idea in the language of the target audience. It maps a concept from one world-view into the experience with which the audience can identify. Once a connection is made between the audience and the presenter, follow-on concepts are much easier to present as the audience has a vested interest in and relationship with the idea being presented. The following two analogies relate computer security issues to concepts in which new students are more likely to be comfortable. Most individuals understand, use and rely on vehicles to meet their transportation needs. While they are likely not auto mechanics or engineers, they all recognize the need for and potential use of vehicles. The same is true with locks.

People interact with locks, choose when to use them, and recognize that different locks are appropriate to protect different assets. They do not need to be expert locksmiths to understand the basics of how a lock functions and how it should be used. The use of these analogies is to bring each student's level of comfort with the new concepts to be consistent with the analogical equivalent. The analogies allow this progression as a sequence of steps, rather than as a new concept.

3.1 Security is Like a Vehicle

Suppose we must communicate the basic notion of "security" to the average person. The definition of "security" depends upon a security policy, and so differs from site to site. We can use an analogy to demonstrate that different sites have different security needs.

Consider someone who needs to buy a new car. What is the best car to buy? The answer depends on the purchaser's needs. If the purchaser is a gardener who needs to haul a lawn mower, wheelbarrow, rakes, shovels, and other gardening tools as well as plants, he will need a pickup truck. A car for a family with five children, on the other hand, needs to hold more people than a pickup truck—perhaps a minivan or station wagon would work. An adventurous soul who enjoys driving off trails in the mountains would get an all-terrain vehicle. So "the best car to buy" is not the same for everyone. It depends upon the intended use.

Even when the purchaser decides upon the type of vehicle, he must select options. Which minivan should the family get? The expensive one has air conditioning; none of the others do. A manual transmission saves $1,000 over an automatic transmission. The Wobbler is very expensive to repair, unlike the Poodle; but the Wobbler's safety record is considerably better than that of the Poodle. All these differences must be considered.

Computer security is like that vehicle. There is no definition that applies to everyone, or every place. Just as different people interpret the idea of "best car", different people and sites interpret "secure" differently.

A writer may consider a computer to be secure if, when the computer crashes, he restarts it and is able to recover what he typed. The writer doesn't connect to the Internet, and never receives electronic mail. So he doesn't worry about people breaking in. But if he loses 10 pages of his latest novel, he will have to reconstruct it, and the result may be substantially less electrifying than the original effort.

A law firm probably defines "secure" along the lines of keeping information secret. The lawyer does not want her clients' secrets available to anyone on the Internet. She wants her clients to be able to talk to her in confidence, so they can be sure the information will remain confidential. Without that confidence, people will stop coming to her firm, and her practice will fail. So this is a good definition of security from her point of view.

But a university has different goals, and so may define "secure" as "only authorized people can change the data on the system". As a university disseminates research results publicly, it doesn't keep its ideas and results secret. But if anyone can change the results of research that the university posts on the web, the research (and

the university) will lose credibility. Thus, this too is an environmentally appropriate definition of “secure”.

Further, if the university adopted the writer’s definition of “secure”, the research results would be inaccessible because the systems would not be connected to the Internet. Similarly, if the lawyer adopted the definition that the university uses, she would lose her livelihood because the client’s information would be visible—but only the lawyer can change it. Just like the notion of a “best car”, the notion of a “secure system” changes with the needs of the user.

As most people either have bought a car, or know people who have, this analogy uses an everyday conundrum (what car to buy?) to illustrate a seemingly unrelated point that most people find difficult to grasp. Rather than follow the technical terms, by equating security to a security policy and then expounding on that concept, it focuses on the heart of the definition: that security is defined differently, for different needs.

3.2 Passwords are Like Door Locks

Let’s consider the effort involved in attempting to convince a group of students that the strength of their passwords is fundamental to protecting their associated digital assets. Many instructors approach the concept of password strength with a discussion of combinatorics. As the instructor delves more deeply into the mathematics of a strong password, students' eyes begin to glaze over. If the importance of password strength has not been presented convincingly, the students are not likely to understand the “why” behind the concept. If students don’t understand the “why”, they are not as likely to be interested in the “how”. An analogy using locks can guide them towards the “why” and increase interest in the “how”.

Most individuals understand that locks vary greatly. In general, the more secure a lock is, the more challenging it is for unauthorized users to gain entry. There is an associated tradeoff as there is also increased difficulty in gaining authorized access. Home bathroom and bedroom doors frequently use privacy function locks. These locks are easy to unlock with a paper clip as they only require pressure applied through a hole in the lock in the doorknob. This is an appropriate strength for a lock in the interior of many homes, where the intent is to protect privacy rather than to protect assets. When choosing a lock for a front door—the main entry to the home—this sort of lock is rarely considered. Homeowners are likely to choose a lock and deadbolt combination that increases the challenge of gaining unauthorized entry. They are willing to face the additional challenges (carrying keys, locking the doors when leaving, etc.) as an acceptable tradeoff for the increased lock strength and associated sense of security. Now we can extend the analogy to an embassy in a hostile area, or a bank vault, and discuss what additional locking mechanisms would be appropriate to protect assets in these cases.

Passwords are like door locks. If someone gains access to your NY Times Online account, you are unlikely to experience a significant violation. Thus a weak password — a privacy lock password — can be appropriate in this case. We can extend the analogy to the password used to log into your online banking system. Now you want a stronger password, as the assets you are protecting are more valuable to you, and

unauthorized access would be viewed as a significant violation. The analogy can even be extended to equate using the same password for many accounts to the using the same key to open all the outside doors in your house. If someone has a key to just one of these doors, then she can open all the doors that use the same lock.

Most individuals will more readily identify with a lock analogy than with the underlying combinatorial mathematics regardless of how nicely is it presented. A good analogy creates a relationship between the concept and the learners and can quickly guide them towards understanding.

4 Challenges

While using analogies provides definite benefits to students, it also poses risks. In some sense, the analogy presents a model of a different situation, framed in a "language" or using concepts that the student understands. The benefit is that the analogy explains the problem in the student's terms. However, any model has discrepancies with the reality it represents, and the student must understand what this delineation. Thus, the point of the analogy must be clear, and the teacher must identify and clarify aspects of the analogy that are based on assumptions. In other words, the teacher must clearly delineate the point at which the analogy (the model) deviates significantly enough to no longer be considered an effective analogy.

Consider the analogy in Section 3.1. The point of the analogy is that the requirements that the "best vehicle" must meet are different; one is for ferrying tools, another for driving a family, a third for off-road travel. This maps into the point that the requirements that the "secure system" are to meet are also different: one preserves data across a system crash, another keeps data from public view, a third prevents unauthorized changes to publicly available data. So, drawing an inference about security from the different needs of the would-be purchasers fits into the model. However, drawing inferences such as there being one specific definition for transporting programs (the gardener driving tools), one for data (the family driving children), and one for miscellaneous uses (the all-terrain vehicles) would be incorrect. So the student must be warned that the analogy does not carry through to comparing the different types of cars to different uses of computers, and the requirements of the purchasers to security requirements.

A good rule of thumb is that the student should find the theme, or the main point, of the analogy and use that, and *only* that, in the inferences drawn. This emphasizes the need for the teacher to make that theme explicitly when presenting the analogy.

As another example, consider the analogy between locks and passwords in Section 3.2. That analogy focuses on the relationship between the lock (password) and the asset being protected. When the protection is for privacy in a situation where someone (a parent) may need to gain access, the lock (password) is weak. When the protection is for security, to protect the things guarded by the lock (the password), the lock (password) is strong. So the student is made aware of the consequences of choosing weak passwords, and can decide under what circumstances to use strong passwords, or to use the same password to protect different things.

The analogy fails when extended to cover other aspects of protection. For example, if the object being protected is a file, the owner of the file can change permissions. But in real life, the owner of the *lock* determines whether access can be changed, by changing the lock. Thus, the heart of the analogy—the equating of strength of the password with the strength of the lock—does not extend to other parallels. The instructor must make this very clear.

One of the greatest challenges in teaching through the use of analogies is coming up with the appropriate analogies that are meaningful to the students and that relate to the course concepts being presented. The experiential diversity of the audience can greatly complicate this effort. Challenges include cultural differences, language barriers, experiential continua, personal biases, and relationship between the instructor and the students.

An example will make this point. On an I.Q. test, students were shown a picture of a cup and asked to identify the object, from a set of 5 pictures, that was most closely related to the cup. The pictures were of a cat, a table, a chair, a saucer, and a kite. Many of the students taking the test selected the table, which was the wrong answer (the saucer was correct). The reason was that the students came from poor backgrounds, where saucers were never used; so they thought the picture of the saucer was a picture of a plate, and chose the table as what they put the cup on.

A faculty member once taught a course in computer security that required students to read Machiavelli's *The Prince*, Sun Tzu's *The Art of War*, and similar books. The point that the faculty member wanted to convey to the students, which he stated explicitly and repeatedly, was that these books showed the reader how to think about systems (military systems, cultural systems, and other societal systems) in order to disrupt, confuse, and ultimately conquer or ruin them. The analogy with how attackers look at sites and systems is clear to anyone who has attacked a system or defended a system. Some students immediately got the point. But other students were so focused on the technical information involved about computer security, they complained that the instructor was turning a technical class into a literature class. Generalizing from books about cultural conflict and manipulation to social engineering and systems analysis was outside their experience.

Key to the use of analogies is the ability of the instructor to determine what the students will relate to. The analogy between the different meanings of security and the different types of automobiles in section 3.1 works with adults who know about cars, especially those who have purchased vehicles. It would not work with children in grade school, though. For them, an analogy involving games or toys would work better, because most children have played games; the analogy could relate the identification of the "best game" to the requirements of security.

Analogies also are affected by cultural norms. Even a concept such as privacy discussed in the lock analogy could potentially have very different meanings to people from Germany (informational self-determination), Japan (constitutional guarantee), and the US (no explicit constitutional right of general privacy). Further, consider an analogy between a system security officer and a police officer. In the United States, where the power of the police is tied to possible violations of the law, the analogy suggests that a system security officer requires some reason to believe that a user is violating the site security policy to monitor the user. In a country where the power of the police includes the ability to monitor people randomly, the analogy

suggests something very different. The key to analogy is to map a new concept to a concept that one understands. If an instructor attempts to maps a concept to a concept that has different meanings for individuals in the class, the understanding of the new concept will be mapped to the diverse worldviews of the students in the class.

5 Conclusion

While a potentially valuable method for identifying with the collective worldview of computer security students, analogies can be tricky. They must be chosen carefully, and explained carefully, because of the associated cultural and societal baggage they may carry. Largely heterogeneous groups are likely to have heterogeneous worldviews. These views are based on assumptions. Likewise, all analogies are founded on assumptions. Further, the assumptions involved are generally not technical. They are human—cultural and societal—and vary with the students' backgrounds. Thus, even in the same class, the students may draw different lessons from the same analogy. This emphasizes the need for the instructor to make explicit the point of the analogy, and also the *limits* of the analogy. Often, the instructor making the analogy is unaware of the assumptions that the students will make. As a result, the analogy fails to teach the students what the instructor believes it should. Thus, there is a failure in the communication network.

While analogies provide an excellent means to map a new concept to the worldview of a learner, this method has some associated challenges. An instructor is a sender who wishes to share an educational message with a student receiver. A good analogy decrypts the message for the student receiver so that the message makes more sense and the student can more easily understand the intent of the message. A poor analogy, or one with which the student receiver cannot identify, effectively encrypts the educational message, making it even more difficult or impossible for the student receiver to understand.

References

1. Definition of Security from Oxford Dictionaries Online. (n.d.). Retrieved February 4, 2011, from http://www.oxforddictionaries.com/definition/security?view=uk
2. Alinsky, S. D., Rules for Radicals. Vantage Books, New York, Mar. 1972.