All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

When should we teach what about cybersecurity to whom?

I recently completed helping to create (although we will be updating it forever) an online high school course in cybersecurity. I think the course is very interesting and hopefully it will be useful in many ways and for many other audiences. But during the development process, and still today as we wrap it up, I am concerned about what we are teaching to whom.

Attack and Defense

Generally, I cannot effectively teach about defending systems without teaching about attacking them. Maybe this is just my limitation, but I suspect it runs deeper than that. Doctors have to know about diseases, but in understanding how to prevent and treat them, they may not need to understand how to give them to people. And yet they do learn about things like germ theory and know which diseases can spread by which means. So in learning what to do to prevent the spread of disease, they also learn how to spread them. That's an example of the need to know about attack in order to defend.

On the other hand, in order to get people sick, you likely do not need to know how to treat and cure them. In fact, in ancient times, biological weapons were used before there was any idea at all about how the diseases might be cured. But be careful here, this analogy is imperfect. In order to be able to create new diseases rather than just spread existing ones, you probably need to know a lot of the same biology as you do to try to find cures for them. So attack, in order to be effective against effective defenses likely needs to know a good deal about defenses.

Need to know

At the most simplistic level, in order to attack or defend against specific targets and attacks (respectively), all you really need to know is what to look for and what to do when you see it. So in this sense, it's stimulus → response behavioral training we need. And that's what a typical security awareness program is typically, and likely should be, about.

Hopefully we still teach our children not to get into a car or, for that matter, go anywhere, with strangers. But any decently trained kidnapper will either use force or start by introducing themselves, so they are no longer a stranger.

> *"Hi, I'm Fred, and you must be [Julie]… your mother said I would find you here, and asked me to giver you an ice cream and take you home for her because she got stuck in traffic." Please substitute the name on the name tag for [Julie].*

There's your attack training. Here's your defense training:

> *"Don't get into a car, or go anywhere, with strangers"*

Of course we could go into unlimited details about what is and is not a stranger, talk about how different sorts of vehicles may be used instead of cars, and so forth. But at the end of the day, training on attack is easier than training on defense, and even though in order to always win you need lots of training on attack, you don't need to always win for attack.

More

To be better at what you do, you need to know more about it. Sure, raw talent helps, but I have found that in most areas, working at it over comes talent except in rare circumstances. Which is to say, if we want to be good at defense, we need to know lots about attack, but not necessarily practice actually doing it (attack) all that much. And to overcome most defenses, we need to know something about them, but we don't need to actually be a defender or practice defending.

On the other hand, it is much easier to lie than detect a lie. And since lying is a large part of attack, it's easier to attack than defend … successfully that is. Until it gets complicated. The more complicated the lie, the easier it is to detect and the harder it is to get right.

Which is to say, in an indirect sort of way, and without adequate basis here, we need to teach defenders about the different ways of lying in order to be successful defenders, while the lack of high quality defenders means we only need to teach attackers a few methods of lying in order for them to be successful.

Getting caught

The punishment for a failed lie is generally very little. But the punishment for failure to detect lies in security can be brutal indeed. When I used to do live physical protection testing, the punishment for being detected trying to get into a facility was just embarrassment at getting caught.

> *The person at the door stops you (verbally) from proceeding past the checkpoint, and you say 'I didn't know' or some such thing, and they send you to somewhere else that you don't actually go to.*

On the other hand, if they don't stop me, I walk into the file room and proceed to look through the files, take pictures, or even originals on paper, and walk out with them. Or I walk through the rest of the building and get into the computer room, wire closets, etc.

The misalignment of punishments is one of the reasons defenders need to know more than attackers in order to be effective.

But how do we know our students are defenders?

Of course we don't. So we teach some attackers and some defenders lots of stuff that we would prefer only defenders know. But on the other hand… why would an attacker bother taking a course in defense? I guess the only ones that would find it worthwhile are the attackers who want to be professional at it. And of course

You can find all of this stuff on the Internet, can't you?

Yes, or course, you can find all the information you get in Medical school on the Internet. And you can also find lots of wrong information there as well. How do you tell the difference? You can test it all out and get the practical experience by practicing medicine on refugees in war zones. Or you could kidnap children by lying to them and practice medicine on them using the Internet guide on how to cure COVID with bleach.

Better yet – just ask the AI about it all. Remember the old saying:

> *To err is human... To really foul things up it takes a computer.*

Back to school

So every time I worry about teaching too much about attacks when I teach about defenses, I remember a few key concepts:

- It's easier to launch an attack than to defend against it
- Any decent attacker can find the attack stuff on the Internet easily
- The punishment for screwing up is almost always less for the attacker
- You cannot really defend well without knowing about attacks
- You can easily attack well without knowing about defenses

I forget the other ones I remember, but I think you get the idea. I am just not worried about attackers who take defense courses to learn how defenders defend against their attacks.

When are they ready for it?

In creating and automating the teaching of the high school level course, I am concerned about the level of sophistication I should be assuming. Thinking back to when I was in high school is probably not helpful, because there was only really one computer used by students in the school, and it was a PDP-8 that I ended up reading the manual for and thereby knowing more about than anyone else in the school. And when I tried to help a teacher teach about computers to younger students, it was using the Basic language (not the advanced version we have today, but really basic Basic), and for the most part, computers were not a big thing.

I have a strong desire not to try to talk down to students, and a strong bent toward not over-simplifying things. When I read some of the stuff folks use to teach people about how computers work, they seem to me like disinformation campaigns aimed at avoiding terms like 'bit' and fail to explain that there is a physical reality underlying the cyber world. One key example I cannot stand is the claim that:

An IP address is a unique number assigned to a computer on the Internet.

Of course this is simply not true. For the skeptics among you, check out 127.0.0.1 or any IP address starting with 10. … Yeah – I know… those don't count… but actually, they do. And by the way, with load balancing devices, and NAT gateways, and Multiple Address Translation, and Onion routing, and invisible routers, and IP tunnels, and so forth, it just isn't so.

I am not afraid to use words that students might have to look up, but we do provide a glossary of terms for terms of art, because when you look them up on the Internet, you get so many different screwy definitions. But I also think it's worth explaining where the use of 'ph' in front of anything ending in 'ing' is just folks making things up because it's popular, and then I explain that all language is pretty much that way. And by the way, "extortion" is the technical term for making people pay you by encrypting their files or threatening to release confidential information.

One other point I should emphasize… I am done with CIA and have been for a long time:

Integrity, availability, confidentiality, use control, accountability, transparency, and custody

There are tradeoffs between them, and all are more or less important depending on the circumstances. We need to stop over-simplifying the basics as early as we can.

Full disclosure

Having said all of that, I am not ready for the full disclosure perspective of handing students (or anyone else), everything they need to carry out a sophisticated (or even not so) attack.

My view of this view began in 1984, shortly before I published my first articles and dis my first presentations on computer viruses based on experiments in November of 1983. That's quite a while ago, of course, and you would think my views would have changed since then. But I stand by them because I thought about them then and have thought about them since, and I still agree with myself (not something I always do of course).

I have never released the original code for the first virus I experimented with, even though by modern standards it would be considered trivial. I think I released the 7 character shell script virus many years ago, and my dissertation committee required that I put some source code in my dissertation.

So the question of what to release to whom and why comes up

To be clear, any virus spreading in the wild is already released, and so is any Trojan horse you got a copy of. And the many billions of malware instances are regularly exchanged by defender companies on an ongoing basis. These folks have a legitimate need to know the information in order to do their jobs, and of course attackers exchange methods all the time.

My issue has to do with what to teach students in classes, and in particular, at the high school level. To me, I see no value in spending their time showing them source code to some complex program that happens to be a computer virus or Trojan or whatever. There are really two reasons behind this.

- If they want to find it, they can do an Internet search or have some AI engine create one for them. It's just like pornography in that way. Easy to find elsewhere and of little educational value at the introductory level (assuming their school covers the same issues). My goal is to expand their minds in terms of understanding cybersecurity.
- It takes a lot of time, and we don't have that much to spare in classes. There are so many things to learn even in an introductory course, that every minute I spend on trying to detail how a program works, is a minute where they don't learn about something more important, like the many different sorts of programs and non-programs that can do the many different things cybersecurity is concerned with.

Full disclosure involves at least two dimensions… breadth and depth. With limited resources and at the introductory level, I prefer to be more disclosing of the breadth of issues than of the depth of any particular issue.

Conclusions

I think we should be teaching cybersecurity to anyone who wants to learn about it, and training everyone on the obvious stuff – like "If it looks to good to be true it probably is". High school students are pretty smart, and should be told the truth in a direct way. Younger kids, age appropriate of course, and grown ups, pretty much like high school students.

I am in favor of full disclosure, in the dimension of breadth over depth. I also like examples that drill down in depth to make the lessons real, and I really like case studies and games for this. But I also value your opinion. So take the course and let me know your thoughts.

