TAG CYBER
LAW JOURNAL
APRIL 2021

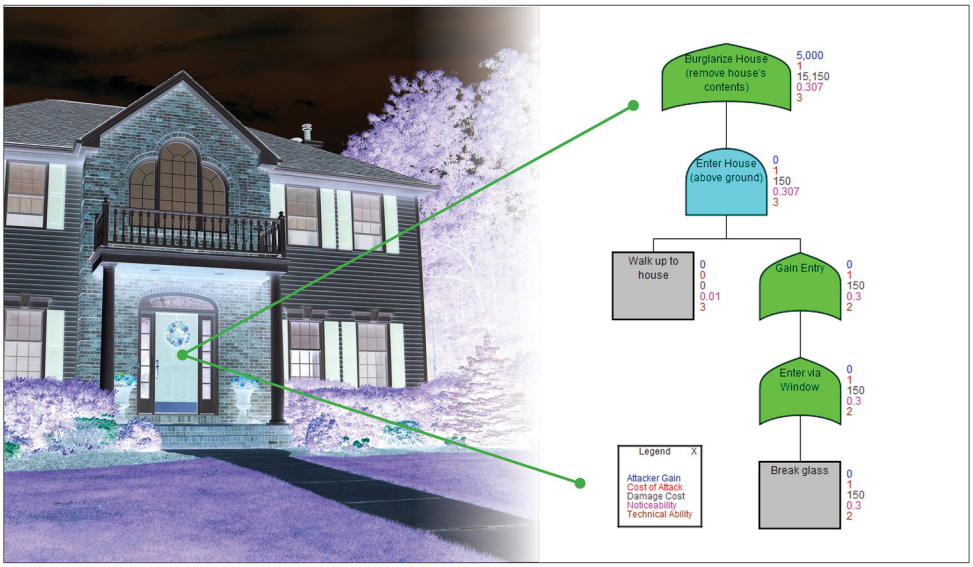
WE NEED MORE SCIENCE IN CYBER SECURITY

How a company created attack tree software that it claims brings rigor to the field.

BY DAVID HECHLER

What struck me first about Terry Ingoldsby's approach to cyber security was the emphasis he placed on objectivity. Everyone knows that working in this area requires a combination of art and science, but Ingoldsby was tired of relying so heavily on the art side. He was a physics major in college, and he was looking for a sturdier foundation—even if it took years to find one (which it did).

As I dug deeper, I realized that his approach also raised important questions about the way companies think about cyber security. Is this a long-term challenge that requires time, attention, and resources from top executives? Or is it a continuing series of potholes that the company must maneuver around on the long information superhighway?



This is how attack tree software would show one way to burglarize a house—and the resources the adversary would use.

When we spoke on Zoom in late March, Ingoldsby first explained why he had hungered for objectivity. He had an analogy he used to explain what he meant. "No engineer worth their salt would ever build a bridge and wonder if it was going to hold," he said. But in essence, that's what professionals in IT security do. "We basically take our current budget and run out and buy stuff, plug it in, and turn it on. And pray that it will do something. And then, when it turns out that it wasn't enough, we get the next year's budget and we go out and buy more stuff."

This is not the way it should be, said Ingoldsby, who is founder and president of Amenaza Technologies in Calgary. (Amenaza is Spanish for "threat" or "menace.") When engineers are commissioned to build a bridge, they gather data. What will its dimensions be? What load must it bear? How many lanes will be required, and how much traffic will it draw? Then they build a model and check it, tweak it, test it. "And only when they're satisfied that the design is correct do they start ordering things and assembling them in accordance with the design," he said.

This is what he wanted to incorporate into his work, and the big thing he was missing was data.

He has a clear recollection of when his quest began. In 1995

he started a consulting company to do system administration and network security for oil companies. He was often asked to undertake security assessments. The reports he produced were probably as good as those written by others in the field, but there was no more rigor to the work, he said, than searching for water with a divining rod. "I probably don't have enough training," he thought. So he signed up for conferences and made the rounds.

Two years later he heard security technologist Bruce Schneier give a talk about attack trees. "Suddenly the lights had come on," he said. The concept involved templates similar to decision trees. It was a way to calculate risk by assessing adversaries' capabilities and your own vulnerabilities. The end result is that attack trees helped you weigh the threat and determine countermeasures to fend off attacks.

Ingoldsby was excited. This seemed to be what he was looking for. After the talk, he approached Schneier and asked if there was software to implement his system. Unfortunately not, the security guru told him.

The next year, Schneier spoke at another conference and Ingoldsby buttonholed him again. Still no software? "No," Schneier told him. "That's why I'm giving these talks. I'm hoping that somebody will go out and write some." That was all Ingoldsby needed to hear. He told Schneier that he would be that somebody. He figured it would take a few weeks. "How hard can this be?"

Ingoldsby smiled before he continued. "Well, that was 20 years ago. And we're still improving and refining the software. So it kind of became my career." A career devoted to selling attack tree software.

A Different Kind of Pitch

Even before he explained how it worked, I could see how different his pitch was from the usual way cyber security is marketed. It's almost the obverse. Nothing about the latest breaches "ripped from the headlines." Or the devastation of a ransomware attack. Usually there's a lot of subjectivity in the pitch. Fear is a powerful persuader.

I asked Ingoldsby about that. "Most security stuff gets sold on fear," he agreed. "I mean, basically put terror in their hearts, and maybe they'll buy something," he said. "From my perspective, if you're ever in the situation where you are now experiencing terror, it's already too late. At best, you're trying to pick up the pieces." The power of an objective approach is clearly an appeal to reason, which may be a harder sell, as Ingoldsby is well aware.

When it comes to sales, there are two big challenges he's run into. What he's selling is not designed to help the IT department fix the most immediate problems they face on any given day. Even when they purchase his software, it won't magically eliminate the to-do list of tasks they need to perform that week. It's a longer term investment. And the benefits of what he offers are likely to be most appealing to company executives and their general counsel rather than the IT department. But he has a hard time reaching them.

This is where I started to see that larger issue emerge. It's one of the biggest challenges in cyber security. So often a crisis comes down to the resources a company had devoted to this area and how much attention its executives have been paying. They may say that cyber is not just an IT problem, but is that reflected in their behavior?

How Attack Trees Work

The Amenaza website has a page devoted to the origin of attack trees. The most important piece was a 1998 paper co-authored by Schneier with research sponsored by the National Security Agency (where two of his co-authors worked). The full picture of their provenance is murky, Ingoldsby said, because they seemed to have been developed in classified environments. In the 1960s, "fault trees" were used to study unexplained missile failures. This seemed to be the earliest version of the concept. Next along the timeline, Edward Amoroso popped up (much to my surprise). The founder and CEO of TAG Cyber wrote about "threat trees" in a 1994 book he published when he was at Bell Labs. Ingoldsby wasn't sure if Amoroso's work was independent of the NSA's, so I asked. Amoroso's answer tied all the trees together. In the 1980s, his work on threat trees involved missiles, just as the earlier fault trees had. Amoroso's work was related to the Star Wars missile defense program (aka the Strategic Defense Initiative). And the NSA was involved, he added.

After securing Schneier's blessing at the second conference, Ingoldsby pulled together a small team to start building the software in late 1998. A few months later, Christine McLellan joined the effort and took charge of software development. The first version of the program, called SecurITree (pronounced secure-i-tree), was born in 2000, and Amenaza Technologies was incorporated in January 2001. Two decades later, McLellan is still there as VP, product development.

Amenaza's business is selling the software. Ingoldsby recommends that customers pay for a three-day training as well. It's not just a matter of memorizing commands. Using the software is a learning experience—almost like taking a course. But it's a different course for every company, because it requires them to explore their own adversaries and their own vulnerabilities. And after the company's employees understand the concepts and how the program works, Ingoldsby usually spends the last day of the training helping them begin mapping their own security landscape.

When he explained the basics to me, Ingoldsby almost sounded like he was describing one of those brainy old board games, like Avalon Hill's Gettysburg. Picture an upside down tree, he said. At the top is the root, which represents the goal the

attacker seeks. Moving down we see processes and procedures that the attacker may adopt to get there. At the bottom are leaf exploits that offer possible ways to begin the voyage.

Attacks require resources. These include money to buy equipment, technical ability, physical access. Assessing them allows a company to calculate the overall cost. And this can be matched with the various types of adversaries to determine whether they're capable of an attack, how much they would benefit from it, and how likely they are to pursue a given path. A company can also calculate the cost to itself and build models that show which paths would be most devastating, and which less so.

Does this make your company secure? Ingoldsby asked and answered the question himself. "SecurITree is a tool in the same sense that Microsoft Excel is a tool," he said. "What does Excel do? If you double click on Excel, there it is in its glory. But it's not doing a thing for you. SecurITree allows you to make sense of what you know. It only reflects back what you tell it. But hopefully the way it reflects it back gives you enlightenment—reveals things to you that you didn't know that you understood."

The Payoff May Not Be Exactly What You Expect

Sometimes those revelations are not what customers expected. A lot of security work involves instinct and gut feelings, Ingoldsby said. And we have a tendency, he continued, to look for the kind of attack we might engineer if we were attacking ourselves. But that doesn't mean the attacker will agree. "So by having to construct this model, it kind of guides one's thinking to look at the bigger picture of how somebody else might take on your system."

One of Ingoldsby's favorite stories involved a client in the defense space. After their three-day training, the attack team returned to a problem they'd been working on for months. It involved military planes, which are apparently most vulnerable when they're sitting on the tarmac—or, in this case, on the decks of aircraft carriers. The group would meet for two hours and get nowhere.

This had been going on for four months. Then they constructed an attack tree to tackle the problem, and they realized what the impediment was. It was the terminology: "Oh, that's what you meant by that? That's not what I meant!" Using the software forced them to describe the attack scheme "in a mathematical fashion," Ingoldsby said, which eliminated the ambiguity. "They made more progress in two hours than they had in the previous four months."

There was one more benefit that Ingoldsby wanted to emphasize. And it's one that would naturally appeal to management and general counsel. In addition to the protections attack trees may help a company construct to protect its IT network, there's another kind of protection it can offer: a due diligence defense. "As you create these models," he noted, "you're essentially creating a document, in a mathematical fashion, of everything you considered and why you discounted certain things as not being a risk. Now, you might be wrong," he conceded, "but you will be able to explain that, 'Based on the knowledge we had at the time, it was a reasonable and rational decision.'"

And for executives and their lawyers, he added, that may be worth a lot.