Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Attacks on information systems - a bedtime story

Once upon a time, there were information systems that were not intentionally attacked, because nobody knew how to attack them. Then the first practical information system was implemented.

Systems have faults

All systems that are realized involve engineering tradeoffs. Those tradeoffs result in limits on the environments in which those systems can reasonably be expected to perform as intended. A designed system is created by people who wish to create it identifying and understanding the relevant operating environments, and designing the system so as to operate properly within that environment. If the system is designed to operate under harsh conditions, where components may fail with substantial consequences, then it typically combined fault intolerance (building it out of components that are more hardy to the expected environmental assaults) and fault tolerance (building it so that as components fail, the overall system continues to operate within the design envelope). These design elements (fault intolerance and fault tolerance) "cover" faults so that they are not realized in system outputs.

Faults may lead to failures

Any realized fault has the potential to lead to a failure unless properly covered by a control of some sort. The nature of the failure depends on the nature of the environment and interdependencies. As a result, it should be reasonably presumed that any fault, unless otherwise and specifically covered, has the potential to produce a failure. The consequences of the failure are, again, context driven, but again should be presumed to allow arbitrary bad things to happen to the system, and by extension, to all interconnected systems, recursively. In essence, history and theory teach us that there is no "minor" flaw when it has the potential to be maliciously exploited.

How faults get intentionally turned into failures

There are and have long been groups of full time professional scientists and engineers who work across multiple disciplines with very large amounts of funding to identify and weaponize information-related exploits. They have, or have available to them, the same education, experience, training, etc. as any and every real person you have ever read about. If you assume anything other than that they will exploit what can be exploited, then you are making a mistake.

These professionals have, over many years of collaborative effort, developed both methods and technologies the make then very efficient at identifying and exploiting faults to their advantage. As an example, they know about the approaches published in the 1970s and 1980s of identifying system inputs that drive a signal to the fault and drive the results of that fault to the output, so as to produce a failure, and they have had technologies developed to automate the process of identifying faults, driving inputs to those faults, and driving outputs

from those faults to desired system effects. In addition, because they have significant resources, they can very often change the operating conditions so that the designed system is no longer operating within the environment it was designed to operate within. This then creates more faults, which themselves can be exploited by the same methods, to produce an increasing range of failures desired by these professionals.

Isn't this science fiction rather than science?

I am sorry to say that this bedtime story is not fiction. It is reality, and it has been reality for at least the last 60 years, and probably longer than that. It was real when the Cold War started, and it continued after the Cold War ended. It was real as information age conflict started to heat up, it is real today, and it will continue to be real for the foreseeable future.

When you read science fiction, these professionals have also read it, or in some cases, they have helped to write it. If you think there is a new possibility that hasn't been explored, you may be right, but chances are you are not. Professionals create and execute plans involving many steps, each of which involves substantial expertise and/or specialized equipment. They design their plans to have multiple paths so that when something goes a bit wrong, they can compensate for it. They are not generally worried about getting caught, and they are not deterred by civil laws, but they very much don't want to be noticed, and generally avoid the spotlight in favor of completing their missions. They don't brag about what they do, or even discuss it outside of the tight-knit group that they operate in. They look like anyone else, earn a living like anyone else. In short, they are professionals.

What can we do about this?

The thing about being a professional is that you spend your time and effort learning about your field of study. Over a period of many years of study and practice, you develop knowledge and skills that support your professional efforts. It is a profession, like being a doctor or a lawyer. If you are going to deal effectively with professionals, you need to start acting like one.

Most of the people I encounter in the information protection field don't really know very much about what they seem to think is their profession. A medical doctor typically studies medicine and their specialty until they are in their late 20s. Then, they practice, typically over a period of many years, until in their late 30's or 40's they become really very good at what they do on a day-to-day basis. They continue to work effectively into their retirement years. Along the way, they continue to take professional education, participate in conferences, many of them write articles on new things they come to learn, and they put forth ongoing effort to stay up to date on their field and their profession. They don't practice in areas where they are not board certified, and when someone asks them a question outside of their actual expertise, they refer the patient to an appropriate expert who knows that particular specialty.

In information protection, if you are going to deal effectively with the "advanced persistent threat", a threat that has been there all along, by the way, you are going to have to become and act like a professional in your specialty. That means gaining knowledge, education, training, skills, and experience, and limiting your work to things you know how to do.

Nighty night, sleep tight, and be prepared!

