Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

How do we measure “security”?

While I await an answer that makes sense, I thought I would point out how we, as engineers, measure other things. I am an electrical engineer (EE) by education, and as a result, I was introduced to fundamentals of certain physical phenomena early in my life. In EE, we have these positive and negative charges associated with different physical things, and we can count the things and their charges, measure them through instrumentation that we calibrate against standards, and use those measurements to make mathematical models of electrical components. With the modeled components, we can build systems and use mathematics to model, analyze, and design systems. We have simple symbols and models for simple systems under normal conditions, like v=ir for a voltage (v) across a resistor (r) with current (I), and more complicated models for more complicated systems under less usual conditions, like the field equations applied to understand propagation of waves through a wave guide.

Essentially every electrical engineer the world understands these same things, uses the same symbols and mathematics, carries out the same calculations, and comes to pretty much the same answers for the same systems. There are similar concepts in other fields of engineering, and they are used to build up mathematical models and understandings which are then applied to design and evaluation of components and composites that form systems, under various operating conditions.

As an engineer by education with a generally scientific bent on things, I figure those in the security engineering community might try to look at security in this light. Unfortunately, there really is very little, if any, community of this sort in the security space, and even less of a community in the information security space. And what community there is, still apparently cannot agree to even the simplest of concepts, like a methodology for evaluating passwords,[1] which have been documented in global use for at least several thousand years.[2][3][4]

I maintain, without substantial basis other than the history of science and engineering in other areas, that this problem stems from a lack of a scientific understanding of the very basic components of “security” in the information arena that we can meaningfully count and the lack of a common language for describing and discussing them. Without this basic set of things, I don't think that meaningful progress is likely to be made, and I don't think that we can reasonably proceed to do engineering in the information security space.

I don't want to be misunderstood in this. I am not saying that people who work in information security don't measure things. To the contrary, they measure lots of things. For example, there is a fad of counting the number of known “vulnerabilities” (whatever that is) in computers, and the number of those vulnerabilities “mitigated” (whatever that is) over a period of time. This is measured by “scanning” for known vulnerabilities using a tool that nobody actually knows how to calibrate (or what it would mean to calibrate it) sold by a commercial vendor who makes money by having different vulnerability lists than other vendors and scanning for them better, faster, cheaper, of which only two can be measured, and only in the simplest of ways.

Indeed there is a whole information security metrics community that has emerged,[5] and as a community, they seem to have largely agreed that they don't want to address any fundamental challenges like developing a theoretical basis for measurement, identifying basic underlying things that might be worth measuring, or providing any sort of mathematical basis for doing anything with the measurements they provide. They seem to be stuck in the challenge of all mysticism before science emerges. They look at things and make up notions about what might be interesting, use the similarity of appearance or descriptive statistics to claim or imply causality when no mechanism has been proposed and scientifically evaluated, and they introduce casual theories that are not evaluated but become part of the urban legend of the field. Attempts to burst these bubbles are met with a level of hostility and frustration, and any attempt to introduce the notions of starting to look at the underlying principles or theoretical issues is met with scorn. Indeed it is easy to become a pariah in that community by bringing up the underlying fallacies of the approaches too often, and if you mention anything serious about developing a physics for the area, don't count on getting any serious attention from the “research” community.

Of course physical security does not have the same set of problems that information security has in this regard. There are some pretty substantial notions underlying physical security and they are widely accepted in the communities that really care about such things. Information security has largely ignored these things, even though they could be quite helpful. For example, physical security measures progress in an attack graph with time as a metric for a physical protective system. They take measurements of different defense mechanisms (e.g., fences, gravel, etc.) relative to specific attack mechanisms (e.g., tanks, people wit tools, etc.) by doing experiments, and form a mathematical model of the overall system by enumerating all of the topological paths from source to target (and back out depending on the issues involved).[6] These are done for different threats identified as part of the threat assessment activity, which also has a scientific basis in facts and measurements, along with an intelligence component, also based on facts.

A similar approach has been taken in scientific experiments with information protection, producing a measurement of progress in an attack graph with time.[7][8][9] Results of these approaches can be used to make design selections and to assess response methodologies (e.g., determine mean time to repair for a desired availability) and thus approach systems engineering. Unfortunately, such approaches have not found their way into the larger information security community, funding to support such scientific development has largely been lacking, and for some reason, there does not appear to be a lot of support for pursuing such lines of enquiry in the larger community. I don't claim that this is the best, or even a good approach, only that it is an approach that has some of the trappings of a scientific basis for an engineering discipline. Notionally, it is at least a place to start thinking.

Returning for a moment to electrical engineering, I recall the first time when working with digital circuits that I encountered the notion of fan-out and fan-in. Here is an example of a design rule that states, in essence, that any output of a digital circuit within the same family can be connected to N inputs within the same family, where N is the fan-out. Instead of having to perform calculations at a detailed level for each time I interconnect two logic gates, I could simply make sure that I stayed within the fan-out (and fan-in) limits, and I was assured that the ultimate implementation would work reliably and within the overall specifications.

The ability to connect one digital circuit to another to form an arbitrary sized overall circuit means that I can design reliably without having to worry about complex interactions ranging across the entire system. Indeed I can connect systems to other systems forming ever larger systems and, assuming I continue to follow appropriate design rules, build up a system of virtually any size, knowing that it will continue to work properly. I may also have some parameters like clock speed and propagation times to concern myself about as a designer, but those too are known parameters of the overall system within the defined operating range of the technology.

In the information security arena I do more or less the same thing when, for example, I design a set of Web servers to support a domain. I know the performance characteristics of the computers, and can measure them reliably in terms of the number of Web pages they can serve over time, the total number of bytes they can server over time, and so forth. As long as each is scaled so that it can handle the maximum bandwidth at the external interface without service failing, I can guarantee against denial of services from excessive requests. If I need more bandwidth, I can set up multiple Web servers, and I can limit bandwidth by limiting the external services rates. I have done this since the middle 1990s, and as a result, despite a wide array of attempts at distributed denial of services attacks against some of my servers, they have never failed from excessive load.

Unfortunately, while some individuals may have such design rules and may have built up limited metrics that they use for internal purposes, publishing results in this arena and making them part of the science and art of information protection seems to out of vogue for now. If as a community we took this sort of approach, we could build up metrics that could be measured reliably with known instrumentation, create designs with known characteristics at their interfaces, and create design rules and the necessary underlying knowledge to build up an engineering discipline that could create systems of systems with known characteristics that could with measurable certainty provide defined protective functions, be calibrated, measured for performance and changes in performance, applied repeatedly to build up larger structures, and produce known and defined operating characteristics over a defined range of operating conditions.

Systems engineers who want effective system security must understand that if the design doesn't treat security like any other design criteria, they will get designs that fail for security reasons. If a systems engineer fails to take into account the operating temperature of space systems, the pressure requirements of underwater systems, or the radiation environment of nuclear safety systems, they get systems that fail when put into use in those environments. The same is true of the security environment. If you plan to put a computer on the Internet, it better be measurably specified and designed for that environment or it will fail. If the operating conditions will change over a range, we better be able to measure and design for them.

So here we sit. As systems engineers, it would be nice to be able to use the same sorts of notions of design for information security as we use for other sorts of design. It would be nice to be able to have standard units of measurement against which we could test things. It would be nice to be able to develop tools for measurement that could be calibrated against the standards, to have a theoretical basis for developing a mathematics and testing it, and then to be able to build up a systems engineering approach to information security like we do in other engineering fields. But first, we need to be able to make meaningful measurements.

References:

[1] In one LinkedIn Internet forum of computer security practitioners, there are almost 1,000 responses to a question of how long a password should be, and there seem to be many different schools of thought on it.

[2] David Kahn. The Codebreakers. Macmillan, 1967.

[3] F. Cohen, "Passwords again - why we can't leave well enough alone", 2009-11, available at: http://all.net/Analyst/2009-11.pdf

[4] F. Cohen, "Change Your Password – Do Si Do", Managing Network Security, Elsevier, September, 1997, also available at: http://all.net/journal/netsec/1997-09.html

[5] See securitymetrics.org and their mailing list for details.

[6] M. Garcia, "The Design and Evaluation of Physical Security Systems", Elsevier, 2001.

[7] F. Cohen, "Simulating Cyber Attacks, Defenses, and Consequences", IFIP TC11, Computers and Security, Volume 18, Number 6, 1999 , pp. 479-518(40) – see an online copy at: http://all.net/journal/ntb/simulate/simulate.html

[8] F. Cohen, et. al. "Red Teaming Experiments with Deception Technologies", available at: http://all.net/journal/deception/RedTeamingExperiments.pdf

[9] F. Cohen and D. Koike, "Leading attackers through attack graphs with deceptions", Computers & Security Volume 22, Issue 5, July 2003, Pages 402-411 – see an online copy at http://all.net/journal/deception/Agraph/Agraph.html