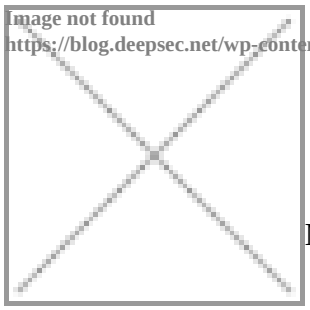
Metrics, Measurement, and Information Security

Posted on **March 28,2018** by **lynx**



Metric is a great word. Depending how you use it, it changes its meaning. The metric of a network path is quite different from the metric system. When it comes to measuring something, the might be an agreement. Why bother? Because we have heard of the term *security metrics* being used for something which should better be called *security statistics*.

In mathematics a metric is a function which tells you the distance between each pair of elements in a set. While this does not necessarily have to do something with distance, it is a fitting analogy. It also connects metric to physics. Measuring how far two points are apart gives you usually a distance (either a straight line or a sum of straight lines). In essence measuring something boils down to comparing your object of interest with a reference. The International System of Units (Système International d'unités) is a good example. The unit, which you are using to express the result of your measurement, has a definition. For example the metre we all (well, almost all of us) are using is defined by the speed of light in vacuum (which is a natural constant). Devices that measure length or distance use this definition. Once you measure something in the real world, it is always a comparison to something else (references are really old). This is true in physics, and it should be true in computer science, too.

Counting is also a form of measurement. Again you use comparisons (your fingers, a herd of cats, collections of stones, visualisations of numbers). Often the number will be bigger than anything you can imagine, but counting is a basic task, so we are used to it. The nice thing about counting is that you can count anything. For example you could count the number of red cars driving past your office, the number of cobblestones on the way to the supermarket, the number of exclamation marks in your Twitter feed, and much more. The problem is that not everything you can count has meaning. Sadly, this is where statistics comes into play. Statistics is really an important branch of mathematics. The methods are as scientific as they can get, and statistical methods work without the real world (which is good, this way they can't introduce a bias). The problem is the application of these principles. You can calculate a lot, just as you can count a lot. Think Big Data. Plus visualisation gives you pretty pictures – but it doesn't give you neither *context* nor *meaning*. This has to come before you start your analysis. That's what I meant by the terms security metrics in the beginning. Picking something you can count and extracting meaning from it can be very hard in information security. We are used to being exposed to all kinds of data. Timestamps, word counts, length of (pass)words follow us throughout our digital lives. Context is the key. Ask anyone who deals with intrusion detection/prevention (called data loss prevention these days).

Back to metrics itself. Be careful with metrics being used to derive a statement about security. We all know the endless benchmarks and performance tests for hardware, software, and everything that is a part of a computer (or a network). It gets a lot worse and a lot more crucial in information security. The number of dropped packets does not equal the number of attacks stopped. The security appliance with the highest throughput might have its reasons for beating the competition. It gets worse when incidents happen.

Don't get caught in the security metrics hype! There is a lot of consulting going on. Databases are being filled. White papers are produced. Cloud(s) cover the sky. Time is wasted. Start with the context. Everything else is bound to fail sooner or later.

If you have somethoughts to share on this matter, please let us know.
Posted in:Discussion,High Entropy,Security | | With 0 comments