Putting the Science into Security – Infosec with Style

Posted on **January 27,2017** by **lynx**

The world of information security is full of publications. It's like being in a maze of twisted little documents, all of them alike. Sometimes these works of art lack structure, deep analysis, or simply reproducibility. Others are perfectly researched, contain (a defence of) arguments, proofs of concept, and solid code or documentation to make a point. Information security is a mixture of different disciplines such as mathematics, physics, computer science, psychology, sociology, linguistics, or history. It's not about computers and networks alone. There is interaction between components. Protocols are involved. Even the simple act of logging in and staying in an active session requires in some parts to talk to each other. And then there are rituals. Scepticism is widespread in information security. Questioning your environment is the way to go, but you need to do it methodically and with evidence-based reasoning.

There is an emotional component to IT security too. „Everything is broken, everyone's going to get hacked eventually.“ You hear this statement a lot, mostly from frustrated engineers. Well, we already know that stuff around us is badly designed or broken by design. Levels of brokenness vary depending on where the stuff (i.e. devices / technology) is being used. Important stuff gets more maintenance and security design than, let's say, your toothbrush. At this point we can veer off and discuss the Internet of Things at length. Unless you methodically lead this discussion based on evidence, please, just don't discuss it. The Internet of Things won't go away just because it is broken (so far). We can handle substances too hot to touch or dangerous chemicals (again, no discussion, we can handle this stuff most of the time), so we can surely deal with dangerous bits. We just have to do it properly. This also means to realise that it is sometimes better to say „I don't know what that means.“ until you have all the facts to decide what you see or hear.

To get the train of thought back on the infosec track, have a look at Hanno Böck's presentation titled „In Search of Evidence-Based IT-Security“. Origin of this talk was the work of Google's Project Zero where the security of anti-virus engines, among other code, was discussed. Confronting the fancy advertising of security products with the fundamentals of theoretical computer science is a good test to see how evidence-based the approach is. Hanno suggests to take a look at the methods used in other fields where things and stuff are also complicated. Randomised controlled trials (RCTs) are an example. While RCTs are not without disadvantages, you don't even find the most basic scientific methods in information security publications. White papers and documents titled "(field) study" are even worse. The lack of gathering facts and to process them scientifically makes information security research vulnerable to manipulation. Infosec people smile when *cyber* attacks are in the news or politicians talk about *cyber* war. That's great, but the shoddy work found in some/many published „results“ leave too much room for ambiguous discussions. We agree with Hanno: „Applying rigorous science to IT security could provide a way out of the security nihilism that dominates the debate so often these days…And by learning from other fields Evidence-Based IT Security could skip the flaws that rife other fields of science.“

DeepSec 2017 will have a stronger focus on academic research in the field of information security. In case you need help improving the scientific approach in your project, please let us know. We might be able to help, and we know a lot of researchers who can also help. Plus there are already results of fine research online and published. Take a look at them. It is much easier to defend claims against the legal department of a vendor. Facts are your friend. Dealing with them correctly will save your day.

Posted in:Discussion,Security | Tagged:Hacking,Mindset,Observation,Research,Science | With 0 comments