All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Confidence in code (or AI)

When I read of the Google Docs “And. And. And. And. And.” failure mode, I again mumbled to myself how pitiful the software industry is and how little confidence we should have in any software.

And. And. And. And. And.?

Yes indeed. Google Docs collapses (or used to) when you put in this and other similar sorts of things. Some one-word capitalized sentences, depending on the words cause the application to stop responding. Some say it’s regular expression analysis→excessive regress. Of course the same is true of some content you put into Google Calendar, and not to push too hard on Google, Microsoft discovered another Unix privilege escalation and published it (might as well bloody Linux when you are being forced by the market to adopt it).

The simplicity principal

I’ve railed on this before, but when we (not me – but the community we) dropped the security requirement for simplicity, we admitted our inability to keep it simple, which is to say, fathomable.

The unfathomability principal

Anything that cannot be understood cannot be secure – or secured.

I just made that up by the way. But it seems to me to be a fundamental concept of dealing with technology. Of course in truth, nothing can be secure. But that’s a different issue I believe I have dealt with in many other articles. The ‘or secured’ component has to do with the less restrictive version of secure in that it is inherently “against” something(s) and an activity you undertake rather than a property of something. Which takes us back to “security is something you do, not something you buy” and related things I have said over the years.

AI AI AI AI AI (as opposed to AI AI captain)

AI cannot be secure or secured when we don’t understand how and why it does what it does. And it’s not enough for the inventor or designer to understand it, because secured is something we all must do and not something the inventor or designer can do for us. AI explainability is something many folks have been seeking for a long time.

The term AI is most current used to describe learning technologies that use high dimensionality statistical proximity matching. But in cyber security, we have used automation for a long time to do many functions, and without them, we would not be able to defend against the high volume of automated attacks. I believe that the vast majority of cyber-security automation is artificial intelligence, in that it automated decision-making. Most of it is readily explainable and explained. And we use it. And for the most part, we can have and reasonably do have confidence that it does what is is intended to do.

Of course it can be bypassed in various ways and of course it is imperfect, but it’s pretty easy to lay out the basic dependencies and fault and failure modes.

Confidence and in confidential

Having confidence is also related to the objectives you are seeking to achieve. If you are aiming at CIA (Confidentiality, Integrity, and Availability) as your objectives, and in that order, you should not have substantial confidence in any software. First off, there is a tradeoff between these three, but more importantly, they are likely not in the right order or the full set of objectives you should be seeking.

Protection Objectives						
Integrity Source	Availability Access	Confidentiality Privacy	Use control Identify	Accountability Attribution	Transparency Process	Custody Source

Our standards of practice[1] identifies Integrity, Availability, Confidentiality, Use control, Accountability, Transparency, and Custody as a fundamental set of protection objectives. And these in the context of the larger model.

Not just your confidence

Confidence is not just about your confidence. It is about the confidence of all the stakeholders that it matters to. If you are in a company, your business depends on the confidence of your customers in your protection. That usually comes from transparency about the relevant issues to their interests. If they think their bank balance is really important to them, integrity and use control related to their bank account are probably high on their list. Transparency with regard to these aspects of protection are key to their trust and confidence, and of course we know that what will be depicted in many cases as transparency will in fact be very opaque claims about integrity and use control.

3rd party review

I recently encountered a potential business partner who, when faced with an actual protection review, decided not to continue in that activity. It seems that undergoing an independent review of security, once they realized what that involved, decided not to do the business. Now imagine if every company required a similar review? Suppose their customers required such a review?

Code review problems

I have written on this quite a bit over time. At a basic level, human code review does not detect intentional alteration very well at all. Automated code review only finds things that can be readily found by regular expression searches and similar techniques (I know this is an over-simplification, but live with it). Learning-based AI techniques will not solve that problem. It's a hard problem – really hard – and all the harder because we have no underlying theory of what it would mean to be "secure", and of course all of these methods that finish in finite time have an unlimited number of false positives, false negatives, or both. By the way, the finite time (and space) restriction is the thing that appears to have created the Google Docs failure.

Conclusions

We cannot reasonably have confidence in code, and should have less confidence as the code becomes more complex and less fathomable. Which means anything complicated will not be secure ever, or secured at least until we figure out what that means. And until we can reasonably list the objectives of security (not just CIA), we cannot even start to discuss the problem in a reasonable way.

1 http://all.net/Arch/index.html Clickable diagram and drill-downs into the standards of practice

