All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Is it secure?

No.

Is that the whole article?

It could be, but I thought I might add just a bit to the answer. I have seen an increase lately in the number of times the term “secure” has been bandied about. Here are a few examples from the media:

> “... is not secure as it may contain unfixed ...”
>
> “... uses a secure server ...”
>
> “... All … is retained on secure servers ...”

What does “secure” even mean?

The first problem with these and many similar ridiculous (and I intend to ridicule them) claims is that they don't seem to have a clue about what the word “secure” means. Interestingly, the dictionary definition has changed over the last 20+ years from “the feeling of safety” to “free from danger or harm”. The latter meaning has long been the definition of “protection”, which has long meant “keeping from harm” or a similar phrase.

So let's suppose that by “secure” they mean “protected” or some such thing – which is to say, kept from harm. As an assertion about anything, such a usage would necessarily imply a context. For example:

> “Secure from general quarters”, which I hear in movies a lot, means something to the effect that “secure or set condition of readiness designated.”[1] while “general quarters” means “All hands man battle stations on the double.” The context here is a set of pre-defined conditions (Set Condition II/III Watch 1/2/3) which can be reached by a defined set of actions.

To say something is “secure” without such a context and as an unconditional would seem to imply that it cannot be harmed in any case. Of course that calls for a clear definition of harm as well. So let's suppose that harm (potentially negative consequences) occurs when services offered by the system are no longer available. Does the uncontexted “secure” means that the system including all of the elements (the users, whatever they are using, and the surrounding relevant environment) can never be destroyed? In most cases I am aware of, the proper application of explosives could produce such harm,[2] and thus the system is not secure in the unlimited sense.

So the term “secure” requires context. But what context?

---

1 http://www.history.navy.mil/library/online/commands_order.htm

2 I have had problems finding an authoritative source of the original quote, which I had the impression was from Alfred Nobel. I found these, among others: “There is no problem which cannot be solved by a suitable application of high explosives.” - William W. Hughes. "There are no problems which cannot be solved by judicious use of high explosives." - British Commando motto, World War 2

Context in terms of objectives and consequences

One of the ways we talk about consequences is in terms of protection objectives. My current list of protection objectives in the generic sense is: integrity, availability, confidentiality, use control, accountability, transparency, and custody. If we assume these as objectives, we might assert that a system is "secure" if it maintains all of these properties to within defined limits, and then make those limits the parameters of "secure". For example, we might say:

- System X is secure against failures in accountability produced by …

But then we could simply remove the "secure" part and say:

- System X has accountability for ...

Another approach is to identify the limits of potential negative consequences. For example, regardless of protection objectives or failures, we might be able to codify the worst case loss.

- System X securely limits losses to $500/day

But then we could also eliminate the "secure" part...

Which is to say, the term "secure" without context is meaningless, and with context, the term is no longer necessary, at least as a noun form (i.e., X is secure).

It's a verb, not a state of being

The underlying problem here is not the word as much as the underlying form of use. Secure is not a state of being. You can "secure from general quarters" by taking a set of actions that move you into a new state from a prior state, but neither state is "secure". You can "secure me a pen" by going and getting a pen for me, although "procure" might be a better term.

"Protection is something you do, not something you buy!"[3] If you prefer the word "secure", feel free, but the issue remains the same. A system is not secure, but it may be "secured" (if you mean by that protected – kept from harm) to the limits of those doing the protection in the context of the threats they face and events that occur.

Actions speak louder than words

History is strewn with failed systems called "secure". I like to point to history in this context because it turns bold claims into realities or dust. Something about refutation and such. One last example – cryptography. I see enormously widespread use of cryptography claimed as the means for security. But most people are apparently unaware that no cryptographic system has withstood close scrutiny for more than about 60 years, and only one time pads (which are often claimed but rarely attained) have lasted that long. Most others have fallen in one form or another in 5-10 years after widespread use. A few have lasted 25 years with only failures at the margins. The requirement for protection of records such as health records is at least the life of the individual. Life spans commonly exceed 80 years.

Summary

I am secure[4] in the knowledge that no system will ever be "secure" and that people will continue to (mis)use the word as if it were meaningful in that context.

3 F. Cohen, "A Short Course on Information Protection in in Personal Computers and Local Area Networks", ASP Press, 1991. (online at: http://all.net/books/pclansec.pdf)

4 I have the feeling of safety...

