

KEYNOTE SPEECH: A Philosophy of Information Assurance¹

Stephen F Bush

I will suggest that society would benefit if universities were to shoulder the burden of creating a “Philosophy of Information Assurance”. While universities have taken the bold step of exploring and teaching Information Assurance along with government, industry and corporations, they are (or should be) in a better position to take a longer, deeper view. Commercial enterprise uses what is believed to be the nuts and bolts of information assurance out of necessity but without adequately considering its true nature. My goal in this talk is simply to pose the need for such a philosophy by asking questions (...and yes, I am cognizant of where Socrates ended up by doing likewise).

One might wonder how we can begin to “implement” information assurance when we have no universally agreed upon definition for information. Remember Theseus’ (black/white) sail message and what happened when Aegeus misunderstood the signal (Aegeus, poor father of Theseus committed suicide needlessly). There was no evil intent, just poor coding of a one-bit message.

If you think information itself has been defined, or is trivial to define, then consider some of the many recently proposed, and un-reconciled, definitions of information. Shannon’s entropy measure (1) is often used in communications; the idea being that the entropy of x is the expected value of its outcome’s surprisal. In simple terms, the more surprised I am that something will happen, the more information is required to tell me about it.

$$I(x) = -\log_2 P(X) \quad (1)$$

An Algorithmic (Kolmogorov Complexity) (2) definition would seem to better capture computational aspects of information because it based on a Universal Turing Machine. In simple terms, if it takes a longer smallest program to represent something, then that thing must be more complex or hold more information.

$$K_U(X|Y) = \min\{|p| : p \in \{0,1\}^*, U(p, Y) = X\} \quad (2)$$

Fisher Information (3) has a statistical flavor, focusing, in a sense, on the sensitivity of the parameters of the maximum likelihood estimate of a distribution’s parameters. It is the amount of information that an observable random variable X carries about an unobservable parameter θ upon which the probability distribution of X depends.

$$I(\Theta) = E \left[\left[\frac{\partial}{\partial \Theta} \ln f(X; \Theta) \right]^2 \right] \quad (3)$$

The future will hold a quantum definition of information (qubits) (4) focusing on efficiency and compression by super-position of classical information.

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (4)$$

Kolmogorov opened the door to a large number of complexity-based definitions of information. The assumption being that greater information content should somehow be more complex and that the length of the smallest description of the information somehow indicates its complexity. Communication Complexity was another interesting complexity measure that looked at the minimum information necessary for distributed users to compute the value of a given function.

¹ NYS Cyber Security Conference: Symposium on Information Assurance, Wednesday, Jun 14, 2006.

My point in presenting these definitions of information is not to discuss them in detail, nor would we have time to do so, but rather to recognize the difficulty in getting our arms around a real definition of information and the implications this has for information assurance. Note that some of the definitions of information are not even computable.

Clearly there are obvious differences between securities of information and security of physical objects. It is difficult for humans to think beyond physical, tangible objects with which we are so familiar. Undoubtedly our bias towards the physical creeps into our understanding and definitions for security. However, let us now make the leap from our total *ignorance* of information itself to our blatant *ignorance* of information assurance.

The pragmatic “nuts and bolts” definition of information assurance is comprised of **availability**, **integrity**, **authentication**, **confidentiality**, and **non-repudiation**. The more you have of these things, the better you are *supposed* to feel. While these characteristics are certainly better than nothing, and provide goals for which implementers can strive, someone, or some institution, should constantly question, refine, and redefine a higher-level view of what information assurance really is; a view that better gets to the heart of defining security and assurance; a philosophy of information assurance.

Put simply, I believe the current definitions and characteristics of assurance do not “get to the heart” of the problem and they are too intertwined with the desirable characteristics of information to be useful. I will discuss each component of the definition of information assurance and ask some naïve and extreme questions.

Availability, while a desirable goal, must admit that processing and resources can be stolen even when used “properly” (e.g. DoS vs. flash crowds). Keeping folks out of my network runs counter to the goal of on-line sales. I would want as many people as possible hitting my site or using my network or products. Perhaps the real underlying meaning of availability is “intent”; I want people who intend to buy hitting my site, or people who intend to use my network for “legitimate” reasons. Words like “legitimate” and “good” are notoriously hard to define in a philosophical sense, much less measure and implement.

If one takes a radical philosophical view and requires that information resources must be used to the greater good of society, then have all designers and implementers of information systems violated availability because they are utilizing resources for a purpose that might have been better used elsewhere?

Integrity, another seemingly desirable goal, can be violated when raw data can be changed without leaving a mark. Clearly, data needs to be modified/changed/processed for legitimate reasons, even for communication.

Again taking a radical philosophical point of view, is error correction coding (which involves changing someone’s information) violating integrity? Certainly the goal is to decode information at the receiving-end resulting in the same data that was sent (this would have helped Theseus’ father Aegeus), but the data was nonetheless changed in the network, most likely without the user’s consent. Certainly the network developer who designed the coding algorithm or implemented coding had good intentions.

Authentication, another assurance goal, can be easily violated because raw data can pass through one’s hands without leaving a mark. This opens the door to anonymity and spoofing. Yet, from an extreme philosophical point of view (I think you are seeing the trend here), the designer has already compromised integrity by passing data from one network component to another, most likely without authentication. By the way, to what level of detail should authentication be required? Should every bit traveling from memory to CPU be authenticated?

Or consider another extreme example, should a good engineer who has not been authenticated, be kept from accessing a power grid’s SCADA network if needed to solve an impending critical problem?

Confidentiality can be easily violated because information can be stolen without being removed (no one can know for sure if it has been stolen). Yet, it is the ease of duplicating information that makes computation so efficient.

Again looking at the extreme philosophical viewpoint, the designer has already compromised confidentiality by allowing machines and perhaps a limited set of people (database managers) to see your data. Is it ok for a machine (no matter how intelligent) to see your data, but not a human? Why? Are humans capable of evil and machines are not?

Non-repudiation can be violated easily because information can be given and received without leaving a physical trace. Again, using our extreme view, the designer has already compromised non-repudiation by allowing hardware and software to exchange information with repudiation.

Each of the definitional components of information assurance differs from its physical security analog and is hard to "assure" because of the very properties of information that make it "efficient" for computation and communication. Certainly, of course, wireless communication has enhanced this problem. Yet, a true philosophical underpinning for information assurance should not be changed by new technology.

A real philosophical component of security continually suggests itself, namely, intent. In other words, one will not care if the currently defined definitional components of information assurance are violated as long as the "violation" (be it the designer/implementer/users or anyone else) is "doing good". Is the operator of a SCADA system that transmits an "abnormal" command to correct a problem compromising the system or doing "good"? Is it ok for machines to read your email, but not people, even if someone reading your email could help you? What is the line between art and crime? Is it all based on intent?

A philosopher, Martin Heidegger mentions that, "*Intention* literally means directing-itself-toward. Every lived experience, every psychic compartment, directs itself toward something. Representing is a representing of something, recalling is a recalling of something, judging is a judging about something, presuming, expecting, hoping, loving, hating – of something." Mark Hammond says in the Philosophy of Intent that "intentionality is that which keeps the mind meaningfully connected to the world it is directed towards. For this reason intentionality has been called the "mark of the mental". Whereas the mind is essentially directed-towards the world, physical phenomena such as tables, chairs, and other inanimate entities are not.

As our world becomes ever more connected and data continuously collected from ever deeper within our physical space, our mental models, or perhaps more rigorously stated, our statistical distributions to which we fit our world, will become ever more accurate, thus ultimately reducing information content (surprisal goes to zero). Put simply, when we can predict what will happen, there is no need for information. At this point, intention should be clear and information assurance will have reached perfection, simply because information will cease to exist. Unfortunately, my line of reasoning here does not help us in the present. I am certain that deeper thinkers and better philosophers would provide us more useful insight.

In conclusion, blindly following the current definition of information assurance will not lead to improved security if the definition is itself flawed. A higher-level, philosophical view must always be present and questioning the foundations of what we take for granted. This is an ideal, but unfulfilled role for university research.