Cybersecurity: From engineering to science

Carl E. Landwehr

Engineers design and build artifacts—bridges, sewers, cars, airplanes, circuits, software—for human purposes. In their quest for function and elegance, they draw on the knowledge of materials, forces, and relationships developed through scientific study, but frequently their pursuit drives them to use materials and methods that go beyond the available scientific basis. Before the underlying science is developed, engineers often invent rules of thumb and best practices that have proven useful, but may not always work. Drawing on historical examples from architecture and navigation, this article considers the progress of engineering and science in the domain of cybersecurity.

Over the past several years, public interest has increased in developing a *science of cybersecurity,* often shortened to *science of security* [1, 2]. In modern culture, and certainly in the world of research, science is seen as having positive value. Things scientific are preferred to things unscientific. A scientific foundation for developing artifacts is seen as a strength. If one invests in research and technology, one would like those investments to be scientifically based or at least to produce scientifically sound (typically meaning reproducible) results.

This yearning for a sound basis that one might use to secure computer and communication systems against a wide range of threats is hardly new. Lampson characterized access control mechanisms in operating systems in 1971, over 40 years ago [3]. Five years later Harrison, Ruzzo, and Ullman analyzed the power of those controls formally [4]. It was 1975 when Bell and LaPadula [5], and Walter, et al. [6], published their respective state-machine based models to specify precisely what was intended by "secure system." These efforts, preceded by the earlier Ware and Anderson reports [7, 8] and succeeded by numerous attempts to build security kernel-based systems on these foundations, aimed to put an end to a perpetual cycle of "penetrate and patch" exercises.

Beginning in the late 1960's, Djikstra and others developed the view of programs as mathematical objects that could and should be proven correct; that is, their outputs should be proven to bear specified relations to their inputs. Proving the correctness of algorithms was difficult enough; proving that programs written in languages with informally defined semantics implemented the algorithms correctly was clearly infeasible without automated help.

In the late 1970's and early 1980's several research groups developed systems aimed at verifying properties of programs. Proving security properties seemed less difficult and therefore more feasible than proving general correctness, and significant research funding flowed into these verification systems in hopes that they would enable sound systems to be built.

This turned out not to be so easy, for several

reasons. One reason is that capturing the meaning of *security* precisely is difficult in itself. In 1985, John McLean's System Z showed how a system might conform to the Bell-LaPadula model yet still lack the security properties its designers intended [9]. In the fall of 1986, Don Good, a developer of verification systems, wrote in an email circulated widely at the time: "I think the time has come for a full-scale redevelopment of the logical foundations of computer security . . ." Subsequent discussions led to a workshop devoted to Computer Security Foundations, inaugurated in 1988, that has met annually since then and led to the founding of *The Journal of Computer Security* a few years later.

All of this is not to say that the foundations for a science of cybersecurity are in place. They are not. But the idea of searching for them is also not new, and it's clear that establishing them is a long-term effort, not something that a sudden infusion of funding is likely to achieve in a short time.

But lack of scientific foundations does not necessarily mean that practical improvements in the state of the art cannot be made. Consider two examples from centuries past:

The Duomo, the Cathedral of Santa Maria Del Fiore, is one of the glories of Florence. At the time the first stone of its foundations was laid in 1294, the birth of Galileo was almost 300 years in the future, and of Newton, 350 years. The science of mechanics did not really exist. Scale models were built and used to guide the cathedral's construction but, at the time the construction began, no one knew how to build a dome of the planned size. Ross King tells the fascinating story of the competition to build the dome, which still stands atop the cathedral more than 500 years after its completion, and of the many innovations embodied both in its design and in the methods used to build it [10]. It is a story of human innovation and what might today be called engineering design, but not one of establishing scientific understanding of architectural principles.

About 200 years later, with the advent of global shipping routes, the problem of determining the East-West position (longitude) of ships had become such an urgent problem that the British Parliament authorized a prize of £20,000 for its solution. It was expected that the solution would come from developments

FIGURE 1. The Duomo, the Cathedral of Santa Maria Del Fiore, is a story of human innovation and what might today be called engineering design, but not one of establishing scientific understanding of architectural principles.

in mathematics and astronomy, and so the Board of Longitude, set up to administer the prize competition, drew heavily on mathematicians and astronomers. In fact, as Dava Sobel engagingly relates, the problem was solved by the development, principally by a single self-taught clockmaker named John Harrison, of mechanical clocks that could keep consistent time even in the challenging shipboard environments of the day [11].

I draw two observations from of these vignettes in relation to the establishment of a science of cybersecurity. The first is that scientific foundations frequently follow, rather than precede, the development of practical, deployable solutions to particular problems. I

claim that most of the large scale software systems on which society today depends have been developed in a fashion that is closer to the construction of the Florence cathedral or Harrison's clocks than to the model of specification and proof espoused by Dijkstra and others. The Internet Engineering Task Force (IETF) motto asserting a belief in "rough consensus and running code" [12] reflects this fundamentally utilitarian approach. This observation is not intended as a criticism either of Dijkstra's approach or that of the IETF. One simply must realize that while the search for the right foundations proceeds, construction will continue.

Second, I would observe that the establishment of proper scientific foundations takes time. As noted earlier, Newton's law of gravitation followed Brunelleschi by centuries and could just as well be traced all the way back to the Greek philosophers. One should not expect that there will be sudden breakthroughs in developing a scientific foundation for cybersecurity, and one shouldn't expect that the quest for scientific foundations will have major near-term effects on the security of systems currently under construction.

What would a scientific foundation for cybersecurity look like? Science can come in several forms, and these may lead to different approaches to a science of cybersecurity [13]. Aristotelian science was one of definition and classification. Perhaps it represents the earliest stage of an observational science, and it is seen here both in attempts to provide a precise characterization of what security means [14] but also in the taxonomies of vulnerabilities and attacks that presently plague the cyberinfrastructure.

A Newtonian science might speak in terms of mass and forces, statics and dynamics. Models of computational cybersecurity based in automata theory and modeling access control and information flow might fall in this category, as well as more general theories of security properties and their composability, as in Clarkson and Schneider's recent work on hyperproperties [15]. A Darwinian science might reflect the pressures of competition, diversity, and selection. Such an orientation might draw on game theory and could model behaviors of populations of machines infected by viruses or participating in botnets, for example. A science drawing on the ideas of prospect theory and behavioral economics developed by Kahneman, Tversky, and others might be used to model risk

FIGURE 2. Scientific foundations frequently follow, rather than precede, the development of practical, deployable solutions to particular problems; for example, mechanical clocks were invented only after determining the longitude of ships had become such an urgent problem that the British Parliament authorized a £20,000 prize for its solution.

perception and decision-making by organizations and individuals [16].

In conclusion, I would like to recall Herbert Simon's distinction of science from engineering in his landmark book, *Sciences of the Artificial* [17]:

> Historically and traditionally, it has been the task of the science disciplines to teach about natural things: how they are and how they work. It has been the task of the engineering schools to teach about artificial things: how to make artifacts that have desired properties and how to design.

From this perspective, Simon develops the idea that engineering schools should develop and teach a *science of design*. Despite the complexity of the artifacts humans have created, it is important to keep in mind that they are indeed artifacts. The community has the ability, if it has the will, to reshape them to better meet its needs. A science of cybersecurity should help people understand how to create artifacts that provide desired computational functions without being vulnerable to relatively trivial attacks and without imposing unacceptable constraints on users or on system performance. ↻

About the author

Carl E. Landwehr is an independent consultant in cybersecurity research. Until recently, he was a senior research scientist for the Institute for Systems Research at the University of Maryland, College Park. He received his BS in engineering and applied science from Yale University and his PhD in computer and communication sciences from the University of Michigan. Following a 23-year research career at the Naval Research Laboratory, he has for the past decade developed and managed research programs at the National Science Foundation and the Advanced Research Development Activity/Defense Technology Office/ Intelligence Advanced Research Projects Activity. He is interested in all aspects of trustworthy computing. In December 2010, he completed a four-year term as editor in chief of *IEEE Security & Privacy Magazine.*

References

[1] Evans D. Workshop report. NSF/IARPA/NSA Workshop on the Science of Security; Nov 2008; Berkeley, CA. Available at: http://sos.cs.virginia.edu/report.pdf

[2] JASON Program Office. Science of cyber-security, 2010. McLean (VA): The Mitre Corporation. Report No.: JSR-10-102. Available at: http://www.fas.org/irp/agency/dod/jason/cyber.pdf

[3] Lampson BW. Protection. In: *Proceedings of the Fifth Princeton Symposium on Information Sciences and Systems;* Mar 1971; Princeton, NJ; p. 437–443. Reprinted in: Operating Systems Review. 1974;8(1):18–24. DOI: 10.1.1.137.1119

[4] Harrison MA, Ruzzo WL, Ullman JD. Protection in operating systems. *Communications of the ACM.* 1976;19(8):461–471. DOI: 10.1145/360303.360333

[5] Walter KG, Ogden WF, Gilligan JM, Schaeffer DD, Schaen SL, Shumway DG. Initial structured specifications for an uncompromisable computer security system, 1975. Hanscom Air Force Base, Bedford (MA): Deputy for Command and Management Systems, Electronic Systems Division (AFSC). Report No.: ESD-TR-75-82, NTIS AD-A022 490.

[6] Bell DE, La Padula L. Secure computer system: Unified exposition and multics interpretation, 1975. Hanscom Air Force Base, Bedford (MA): Deputy for Command and Management Systems, Electronic Systems Division (AFSC). Report No.: ESD-TR-75-306, DTIC AD-A023588. Available at: http://nob.cs.ucdavis.edu/history/papers/bell76.pdf

[7] Ware W. Security controls for computer systems: Report of Defense Science Board task force on computer security, 1970. Washington (DC): The Rand Coporation for the Office of the Director of Defense Research and Engineering. Report No.: R609-1. Available at: http://nob.cs.ucdavis.edu/history/papers/ware70.pdf

[8] Anderson JP. Computer security technology planning study, 1972. L.G. Hanscom Field, Bedford (MA): Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC). Report No.: ESD-TR-73-51, Vol. I, NTIS AD-758 206. Available at: http://nob.cs.ucdavis.edu/history/papers/ande72a.pdf

[9] McLean J. A comment on the 'Basic Security Theorem' of Bell and LaPadula. *Information Processing Letters.* 1985;20(2):6770. DOI: 10.1016/0020-0190(85)90065-1

[10] King R. *Brunelleschi's Dome: How a Renaissance Genius Reinvented Architecture.* New York (NY): Walker Publishing Company; 2000. ISBN 13: 978-0-802-71366-7

[11] Sobel D. *Longitude: The True Story of a Lone Genius Who Solved the Greatest Scientific Problem of His Time.* New York (NY): Walker Publishing Company; 1995. ISBN 10: 0-802-79967-1

[12] Hoffman P, Harris S. The Tao of IETF: A novice's guide to the Internet Engineering Task Force. Network Working Group, The Internet Society. RFC 4677, 2006. Available at: http://www.rfc-editor.org/rfc/rfc4677.txt

[13] Cybenko G. *Personal communication,* Spring, 2010. Note: I am indebted to George Cybenko for this observation and the subsequent four categories.

[14] Avizienis A, Laprie JC, Randell B, Landwehr C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing.* 2004;1(1):11–33. DOI: 10.1109/TDSC.2004.2

[15] Clarkson MR, Schneider FB. Hyperproperties. *Journal of Computer Security.* 2010;18(6):1157–1210. DOI: 10.3233/JCS-2009-0393

[16] Kahneman D, Tversky A. Prospect theory: An analysis of decision under risk. *Econometrica.* 1979;47(2):263–291. DOI: 10.2307/1914185

[17] Simon HA. *Sciences of the Artificial.* 3rd ed. Cambridge (MA): MIT Press; 1996. ISBN 13: 978-0-262-69191-8