UW Computer Security Research and Course Blog

How to *think* like a security professional

By Tadayoshi Kohno at 2:13 pm on November 22, 2007 | 9 Comments

Why this blog. A computer security course should teach you many things. You should obviously learn the important technical material, including aspects of applied cryptography, programming language security, web security, and so on. We'll cover many of these technical concepts in the lectures, homeworks, and projects.

But a key goal of my courses is to help you learn more than just the technical material. My goal is to help you cultivate *the security mindset* and to help you become *mature security thinkers*. This blog plays a critical role in achieving these goals.

The security mindset. If you're new to security, you're probably wondering what I mean by *the security mindset*. Let me give you a brief example. Suppose you see an advertisement for a brand new product — the Miracle Foo. Is your first reaction:

> "Wow, the Miracle Foo is a cool product, I can't wait to use it?"

Or is your first reaction:

> "Wow, the Miracle Foo is neat, but *I wonder if someone could subvert the security or privacy of* the Miracle Foo *by doing Blah*?"

If you're immediate reaction is the latter — and especially if you've filled in the blanks for "*by doing Blah*" — then you probably already have the security mindset, or at least the makings of that mindset. If not, don't worry! This mindset is *not* natural for most people. It requires you to think like an adversary — to be constantly thinking about how a malicious party might circumvent the goals of a system or product. This blog will help you develop that mindset. Never again will you see a product advertisement and not wonder what mischievous things an adversary might be able to do.

Why cultivating the security mindset is important. You may someday find yourself working on the design, implementation, or evaluation of new computer software or hardware systems. If you have the security mindset, then you will be better able to identify potential security problems with the systems on which you are working. You may not be able to fix all of the security problems by yourself, but you'll still know that the problems exist and will be able to get others to help you fix the problems. But if you don't have the security mindset, you may never realize that your system might have security problems and, therefore, obviously can't protect against those problems in a principled way.

Furthermore, technologies change very rapidly, which means that some of the technologies and topics that I cover in my courses will inevitably be out-of-date in 10 years. But if I can help you learn how to *think* about security issues and have an appreciation for adversaries, then you can take that *security mindset* with you for the rest of your life and apply it to new technologies as they evolve.

Broader perspective and becoming a mature security thinker. There are many other things to gain from this blog as well. As some of you may know, my personal research interacts broadly with policy, law, medicine, ethics, and so on. Given my experiences, I believe that it is critical for you to understand how technologies

interact with the "bigger picture" and society at large. This blog will give you an opportunity to reflect on the "big picture" issues surrounding technology and society.

Filed under: Announcements — 9 Comments »

9 Comments

- 1

Comment by mark pringle

March 20, 2008 @ 12:28 am

The increased need for security in the present era is concomitant with the emerging need for greater protective stability in a gross national product driven postmodern economy-of-scale corporate economy.

The challenge is to maintain optimal individual freedom while obtaining maximal security; hence a degree of compartmentalization is required in the intelligence effort in order to avoid the acceptance of regimes condoning the direct use of force in lieu of a more circumspect approach to management of untoward and potentially conflagrative circumstances.

As a result, the capacity required for such cognitively based approaches to security, are necessarily fraught the same dangers one would anticipate resulting from failure to insulate adequately dangerous matters of intelligence from the opposition (real or envisioned). It is certainly to be expected that the evolution of security measures and training in the present age of non-nation-state encapsulated conflict should lead to innovative research surrounding the cognitive aspect of predictive security; however the adoptation of a particular mode of education as a new modern political institution (Machiavelli's 'intitutions' being the basis of the modern state) is merely the initial step (for it is not fully adequate in itself) toward understanding the modern security problem in toto.

The problem itself is of course as anceint as politics; however, the process of civilization has been able to accommodate quickly enough at each new turn without resorting to a completely militaristically polarized form of governance; and the hope to retain this grace for the modern era is presently challenged as it never was before by the recent emergence of a third modern cofactor to the pre-existing cofactors inherited from the cold war era (weapons of mass destruction & the WOMD-driven geometric proliferation of competitive intelligence efforts): the establishment of a global hegemony, i.e. Mr. Fukuyama's "End of History."

The realization of this latter factor, while being both beneficial and relatively benign, does not make immediately make manifest the consequent change in the framing of poltical militaristic conflict in the present era, nor does it make manifest the implications of said change; what is consequent is the shift from more predictable localized conflict to non-localized conflict, driven by decentralized intelligence sources, fueled by increasingly more dangerous weapons of mass destruction, and pregnant with the absolute necessity of urgency of the latter.

The consequences are far-reaching indeed. Moreso than might initially be imagined; however there is hope in the institutionalization of such congnitive methods. For while intellect may spring up naturally in the wild, its allegiance may be to some degree naturally suspect, for which reason it is more cautious to implement such measures.

I can only hope that the casualties amongst those whose creative facutlies were unpredicted, unexpected, and undesired will be few. Rare gems cannot be manufactured; neither can human beings. Where would