File 20100616.0650: Notes from reading group this morning:

The paper discussed was 'The Ten Best Practices for Secure Software Development' by Mano Paul (Vienna, Virginia: International Information Systems Security Certification Consortium (ISC)$^2$, undated).

Cornelius provided the Skype connection. I heard John, Ivan, Cornelius, Shamal, Mingqiu, Ronald on the call. The purpose of this white paper is to convince managers to buy (ISC)$^2$ training for their departments in order to tick a list for their upper management showing that they have exercised due diligence. The group did not know much about security certifications; I said that they serve three purposes: for individuals, to get hired. For managers, to show to their higher ups (or to regulators) that they have exercised due diligence. For US defence contractors, to satisfy DOD 8570.1 workforce improvement programme requirements.

Ivan said that it was surprising to him that 8570.1 pays no attention to university degrees. I confirmed that it does not.

Here is what I said in an email afterwards:

> From the perspective of US defence contractors, certifications are a big deal.
>
> US Department of Defence directive 8570.1 requires all personnel with privileged access to DoD systems or any sort of software development responsibilities to be certified by the end of calendar year 2010. This affects more than 100,000 people. So far, compliance ranges from 25 to 40 percent amongst some contractors and parts of DoD, with a few military units at 100 percent. The deadline has been extended a few times but we are told that no extensions will be given after December 2010.
>
> The acceptable certifications are: A+, Network+, SSCP, CAP, GISF, GSLC, or Security+ for entry-level personnel; GSEC, SCNP, CISM, or CISSP for mid-experience level (5 years), and CISA, CISM, or CISSP are required for senior people. Certain operations personnel will be allowed to substitute the Certified Ethical Hacker (CEH), although to say that one is controversial would be an understatement. The CISSP requires a university degree, although experience can be substituted in some cases.
>
> After 8570.1 goes into effect, the only people allowed to perform security engineering or architecture functions will be those holding one of the advanced certifications beyond the CISSP, called ISSEP, ISSAP, and ISSMP. To sit the advanced exams, a person must already have held a CISSP for at least two years.
>
> These certifications have three uses: for individuals, they can get a person hired. For department managers, they are countable tokens useful for demonstrating to upper management that due diligence in hiring and training with respect to security has been done. Finally, for US defence contractors, they are required to satisfy 8570.1.

Note that university degrees in security are not counted at all.

# References