2d Lt James Marvin

Seven Pernicious Kingdoms Review

This article furthers our discussion on education tools for security minded developers and individuals. This tool is more of a mindset than a game. Tsipenyuk, Chess, and McGraw want to illuminate developers with what they call a taxonomy. You may recall a taxonomy from you Biology class in high school where we used a taxonomy to group the various species on the planet. They want to group software security errors in a similar way. The groups they came up with were input validation, API abuse, security features, time and state, errors, code quality, encapsulation and environment (Tsipenyuk). They did this because previous classification methods “focus[ed] on classifying operating-systems-related security defects rather than the errors in software security” (Tsipenyuk). They hoped that this new taxonomy would be written with more “practical language centered on programming concepts” and be more useful to the developers trying to design with security in mind (Tsipenyuk). This scheme allows developers to organize their security concerns and make goals concerning the performance of their software with respect to the seven phyla. We should care about this because as developers or cyber program managers we will need to lead security reviews for our software. Organizing the possible errors in a manner like this can be helpful for breaking down the overall problem of security into smaller problems.

Tsipenyuk et al., “Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors”, 2005