File 20101118.1600: Notes from the new Engineering meeting this afternoon (normally scheduled for 10:00 a.m. to 10:30 a.m. Thursday mornings). The 5.01 patch is being prepped and tested by the developer. In addition they are developing a new process for rating maintenance. Under the TCSEC and later the Common Criteria, maintenance of evaluated products based on COTS hardware and operating systems, especially network-facing systems, was invariably an area of contention amongst developers, certifiers, and vendors of the COTS operating systems integrated into evaluated products. The RM developer has seen the problem become only more acute with the increasingly common integration of COTS and FOSS software components into the evaluated baseline as subsystems—e.g., anti-virus, malware scanners, user interface libraries, SSL libraries, LDAP libraries, and database libraries. The issue, in the developer's view, is the extent of the TCB. For Rating Maintenance Phase (RMP) reasons, it is strongly in the developer's interest to define any component that the developer depends on another developer for to be outside the TCB so that asynchronous patches and security updates will not trigger recertification. This has been a chronic problem for the RM developer since at least 1998 when the developer first ported the application to an evaluated OS that was actively in RMP under TCSEC. Around 2000, the OS vendor shifted to CC evaluation but was never very good about defining a solid process for reconciling security patches with the evaluated configuration. Consequently, the developer was forced to define its own process and solicit approval from numerous (at the time) U.S. government agencies in order to maintain its certification and accreditation—completely separate from the certification status of the OS, another thing absolutely necessary for NSTISSP No. 11 compliance. The solution never was completely satisfactory, but was tolerated implicitly by a series of programme offices and by NSA because all were aware that no superior solution was forthcoming at the time.

The interesting thing this week is that the RM developer is proposing a new solution. The 'OSP' patch concept will separate FOSS and COTS patches and security updates for the first time into a regular outside-the-TCB patch cycle independent of application-level TCB changes, run on a regular schedule that accommodates COTS and FOSS vendor/developer patch cycles. The OSP rate of change will be independent of TCB patches and itself is divided into several categories, each with its own independent and displayed version number. The developer is proposing this solution to the problem of keeping COTS and FOSS components—to include OS security updates, patches, and hardware firmware updates—including non-security-critical OS components to the certifiers in the course of RM 5.0 SABI deliberations of the CDTAB and DSAWG. This is an important development and represents in my view a significant advance over the previous mode of operation of CDS developers. It shows a recognition by the developer and presumably the programme office of how the world actually works as opposed to how the standards say it should work. It is unclear whether the OSP proposal was initiated at the behest of the developer's engineering organisation, IV&V, certifier or programme office but the document is now travelling in the direction from the developer to the programme office. The new process, if approved, will allow the developer to respond more quickly to IAVAs and will improve compliance, something monitored by agencies other than the programme office sponsor, certification authority, accrediting authorities and data owners.

I obtained a look at the developer's roadmap for post-5.0 CDS improvement, and noted that the planned progression of 5.01 through 5.02, 5.1, 5.2 and 6.0 versions closely matches the programme office sponsor's COTR presentation to agency management of 5.1, 5.2 and 6.0 versions. The feature sets agree, not surprising given that they are negotiated between the programme office and developer according to what the engineering organisation beleives is technically achievable. The next major revision of the CDS, designated 5.1, will have a completely overhauled HCI although user-visible changes will be minimal. Underneath, the implementation will have completely changed. The roadmap does not indicate recertification trigger points although I have suggested that to the developer as an improvement.

References