File 20100325.2008: Notes for paper:

Unsteady Ground: Certification to Unstable Criteria

What happens when a system that has been developed successfully under one particular set of security testing criteria suddenly finds itself having to conform to a completely new set of rules? The question is not hypothetical; the situation arises whenever a new certification scheme is adopted, eg the Common Criteria for Information Technology Security Evaluation throughout its various revisions, or regularly as clockwork as in the case of a peculiar species known as Cross Domain Systems (CDS). Lack of communication amongst certain U.S. government agencies leads to unnecessary duplication of effort and multiplication of cost with no concomitant improvement in security, as will be shown below.

Background of the Problem:

CDS are unique in that they often encounter new security criteria. By definition, CDS installations always span at least one boundary between security domains controlled by different data owners. Data owners usually do not trust one another with access to their data, hence the need for a controlled interface between the security enclaves. A typical example of a CDS application would be a one-way interface allowing wire service news articles to flow into a classified intelligence gathering system. The data owner of the classified system worries about two potential threats: accidental spillage of classified information into the unclassified news wire, and the potential for introducing malicious code into the classified system from an outside source.

The previous example is simplistic because it presumes a unidirectional flow of information from low to high (unclassified to classified). More realistic CDS installations must be able to cope with bidirectional flows, such as a web browser inside the security enclave that needs be able to do searches of unclassified databases outside. In practice, multi-directional information flow requirements are not uncommon. Depending on the capability of the CDS, one system might handle scores of channels simultaneously, interconnecting more than a pair of security domains at widely different classification levels. Internally, the CDS maintains separation of information by classification and source, routing inputs to outputs according to rule sets specified by the data owners. Advanced CDS systems have the capability to transform data in flight, whether by transliterating message formats or by sanitising classified information for release at a lower security level.

Thus, as a result of inherent complexity CDS present a uniquely high risk of failure whilst at the same time having the potential to cause a great deal of damage to national security. Consequently, they are developed and tested with utmost care. Assurance begins with formalised requirements and specification reviews, proceeding through software development accompanied by systems and security engineering, vetting of programme personnel, design and code inspections, unit and system level testing, configuration management of software and hardware, documentation, training of installers and operators, audits, and process improvement.

Once development is complete, Certification Test and Evaluation (CT&E) begins. The question of who writes the test procedures is interesting. In practice, the developer (being most familiar with the system) always creates an initial set of tests and expected results based on Factory Acceptance Test (FAT) procedures. Then a different organisation uses those procedures to perform Independent Verification and Validation (IV&V) testing. At each stage in the testing process, 'findings' (deviations from expected results) are reported. Findings are categorised by severity: Category I findings are show-stoppers. Category II findings are less severe but must be corrected before CT&E can proceed to completion. Category III findings would not necessarily prevent certification and fixing them may be deferred for up to 180 days. Category IV findings are minor and could be deferred indefinitely.

After CT&E, each instance of the CDS must be installed and accredited for a particular purpose in a particular location. After the initial site survey, a trained installer configures rule sets in coordination with all data owners involved and installs the system in the location where it is to be used, but not connected to all of the network endpoints. At this point, site operations personnel, system administrators, and security officers are trained on the new system. Before the CDS is allowed to connect for the first time, it must be tested one more time in a process known as Security Test and Evaluation (ST&E). Since the ultimate purpose of a CDS is to reduce residual risk to a level acceptable by the data owner(s), the Designated Approving Authority (DAA) is a person delegated by the Principal Approving Authority (PAA) of the data owner formally to accept responsibility for all residual risk in the operation of the CDS. IV&V personnel assist the DAA with ST&E by exercising the CDS through test procedures until the DAA is satisfied and agrees to accept responsibility for the residual risk. The DAA then issues an Approval to Connect (ATC) and allows the system to operate. Approval to Operate (ATO) is for a

limited time—no more than three years—and contingent on security-relevant changes not being made to the system without the approval of the DAA.

The Problem:

All of the aforementioned steps are necessary to guarantee the level of assurance needed for a modern CDS. But at this point we argue that the process loses coherence. It was mentioned earlier that data owners typically do not trust other data owners, at least not completely. With multiple data owners come multiple DAAs. With multiple DAAs come repeated rounds of ST&E, typically conducted by the same IV&V personnel—being familiar with the system—and using similar or identical test procedures.

Repeated testing to the same or similar criteria by different agencies of the U.S. government seem to be conflating the principle of defence-in-depth with the practice of IV&V.

Further, it is...(evidence and preliminary results go here)

Proposed Solution:

Security accreditation of classified U.S. government IT systems, particularly those involving CDS, comes down to a relatively small number of people. Historically, the reason why they are not already in communication is because of compartmentalisation.

Summary and Conclusion:

The problem can be solved by facilitating communication amongst DAAs representing different data owners.

NOTE: refer to 800-53 and 800-37 for definitions of CT&E and Cat I, II, III, and IV findings. Missing citations!

Still to be described, and lacking in the above narrative are my evidence for the existence of a problem and details of the proposed solution. I have boiled down the description of CDS and software development assurance to the smallest amount of text I can but I keep running into the six-page limit for this conference. I have to explain what CDS are—to an audience not familiar with them—or the nature of the problem doesn't make sense. Still working on writing it.

safety critical standards

time a major revision is made to the

and regularly in the case of one particular class of software known as Cross Domain Systems (CDS).

times when it occurs: CC introduction, CC revisions, DCID 6/3 to NIST SP 800-53 transition

times when it does not occur: when the developer chooses not to submit for re-evaluation under the new criteria; when installed systems are not re-tested; when systems already in development under ongoing contracts are 'grandfathered in' under the old rules.

References