
UK IT SECURITY EVALUATION & CERTIFICATION SCHEME

UK CC Interpretation - UK/2.3/005

1 March 2007

Status: Endorsed for use in UK Scheme

Subject: SOF-medium Rating for Passwords

REFERENCES CEM, Version 2.3, August 2005 - Annex A.8

Issue

1. If Tables 3 and 4 in CEM are used to calculate the SOF rating for a password mechanism, where automated attack is not possible (i.e. Equipment = None in Table 3), then it is impossible for the resultant SOF rating to be SOF-medium.
2. This is because the attack scenario that needs to be considered is that of a layman manually attacking the password mechanism. Assuming no knowledge of the TOE is needed, and no equipment is used, the SOF rating is dependent purely on the time taken to defeat the mechanism. If elapsed time and access to the TOE is > 1 month, then this achieves a score of 17 (8 + 9). According to Table 4 this is only SOF-basic (18 is needed for SOF-medium).
3. The only way a higher SOF rating can be achieved is if the time taken is deemed to be "Not practical". According to Table 3, the rating achieves SOF-high.
4. Therefore, literal application of the SOF tables to purely manual attacks can only ever result in a rating of SOF-basic or SOF-high. This seems unreasonable, and surely was not intended by the CEM authors. For example, if the said layman is attempting to defeat a password mechanism, every hour of every working day, and is still persisting with the attack over a month later, can one seriously characterise this individual as having "low motivation" and hence having low attack potential (cf. the SOF-basic definition in the CC)?

Interpretation

5. SOF ratings calculated using the guidance in CEM A.8.2 should always be validated against the definitions of the SOF rating levels as given in CC. In particular, if manual attack is the only attack scenario being considered, then careful consideration should be given if the time required is greater than 1 month. If the time taken is insufficiently great to be judged as "Not practical", a SOF rating of SOF-medium may still be justified for any of the following reasons:
 - a) In practice, any manual attack taking greater than 1 month would be systematic rather than random. To execute a systematic attack over this period would probably require some form of automated support (e.g. to generate a list of passwords to try), or may require a "proficient" attacker to be able to decide which passwords to try in a systematic manner. Either consideration would lead to an additional 2 points for either "standard equipment" or "proficient" expertise.
 - b) If the time is significantly greater than 1 month (e.g. 3 months or more) then the principle of interpolation of table values given in CEM para 1831 could be extended to justify the additional point necessary to achieve SOF-medium.
 - c) In the attack scenario described, attack is likely to be through the normal login process, where failed login attempts may be audited. Thus the attack is likely to be detected, in which case (following CEM para 1836) the higher rating of SOF-medium would be justified.