Introduction to Security 2004 – Paper 3 Question 9 (MGK)

(*a*) Cryptographic keys should be generated with a secure random bit-sequence generator. Its output must not only be statistically indistinguishable from true random bits, it must also be completely unpredictable for an attacker. Suitable sources for unpredictable bits in desktop computers include secure hash values of hundreds of concatenated high-resolution timestamps of input/output interrupts, including keystrokes and mouse movements. These can be used directly as keys, or if a higher bitrate is required, they can seed or key a secure pseudo-random bit-sequence generator (e.g., as used in stream ciphers such as the OFB or CNT modes of operation of a block cipher).

(*b*) Memory can be overwritten (zeroized) with a constant value when it is reallocated to a new user, or immediately after it has been deallocated by the previous user. The first approach protects against attackers who look in readable memory obtained from the operating system for data stored there by previous users. The second approach protects against attackers who can bypass the operating system when accessing the memory (e.g., by directly reading a stolen harddisk).

(*c*) (*i*) Write access to the parent directory is necessary and sufficient to remove a file. Subdirectories must also be empty before they can be removed.

(*ii*) In a parent directory with the "sticky bit" set, files and subdirectories can only be removed by their owner, even if others have write access to the parent directory.

(*iii*) Place the file into a subdirectory to which only the owner has write access. This subdirectory cannot be removed by anyone else as long as it is not empty, even with write access to its parent directory.

(*d*) For the 6-digit decimal code of the VS100, there are 10^6 combinations. An attacker will succeed on average after trying half of these, and therefore has to enter on average $6 \times 10^6/2 = 3 \times 10^6$ digits. The VS110 expects the entry of eight 5-digit passwords, each of which can be guessed in $10^5/2$ attempts. The attacker can therefore open the VS110 in only $8 \times 10^5/2 = 4 \times 10^5$ attempts and therefore has to enter on average $5 \times 4 \times 10^5 = 2 \times 10^6$ digits. The more expensive government version VS110 can actually be broken faster.

[The questions relate to (a) random number generation (lecture on symmetric cryptography), (b) operating system security functions (lecture on operating system and network security), (c) discretionary access control in POSIX (lecture on access control), and (d) passwords (lecture on authentication techniques).]