Security (code) related experience (dam-security)

David Morano
david.a.morano@gmail.com
1(781) 388-1799

Some selected software experience related to security and code safety is highlighted with these notes.

+ written SETUID/SETGID program
    - drop privilege after required use
    - write it to be SETUID to a lower privileged user to begin with
    - UTMPX update (refactored)
    - PTY ownership change (refactored)
    - DMAIL - mail delivery

+ network related code needs to guard against spurious input
    - classic input buffer overruns
    - no use of STDIO |gets|, use |fgets| instead
    - all programs receiving input need to guard against bad input

+ servers do not need to be privileged to acquire privilege
    - call a special SETUID program to acquire privilege and then
    pass the file-descriptor back to the server (|openport(3dam)|)
    - TCPMUXD - network listen server and sister family of servers
    - DTCMHS - Common Desktop Environment (CDE) calendar entry query
    - COMSAT - mail notification

+ string management subroutines to only operate on counted strings

  sncpyxxx()
  snwcpyxxx()
  strdcpyxx()
  mkpathx()
  mknpathx()

+ use C++ |vector| and |string| objects and other STL containers

+ limit input or acquired strings to largest reasonable amount to protext against resource exhaustion
    - mail message header fields (too long)

+ I have also written some Pluggable Authentication Modules (PAM) shared-objects
    - enhanced RSH and RLOGIN PAM module to ignore "#" commented lines
    - log reporting of access

+ general buffer management code
    - memory allocation and free auditing and tracking (uc_memalloc)

+ embedded real-time coding (inside telecomm equipment)

+ enhanced an early version of the Secure Login daemon (slogind)
    - added additional optional keys to get a valid authentication
    - added additional environment to the spawned process