secure programming in C

fonti di input convenzionali e atipiche

- standard input
- parametri sulla linea di comando
  - nome dell'eseguibile: argv[0]
- variabili di ambiente
- form di input nei programmi interattivi
- link dinamico di librerie
- directory corrente del processo
- files
- inter process communication, ecc...
- rete (socket)

buffer overflow: funzioni standard

alcune funzioni standard che possono provocare buffer overflow sono

- strcpy()
- strcat()
- sprintf()
- gets()
- scanf() (%s)

vedi sezione 3 dei man unix

buffer overflow: funzioni standard

da usare

- strncpy()
  - attenzione non sempre inserisce il byte zero alla fine
- strncat()
- snprintf()
  - attenzione su vecchi sistemi può essere identico a sprintf()!
  - vedi i vecchi linux con Linux libc4
- fgets()
  - attenzione al byte zero di fine stringa!

buffer overflow: funzioni standard

realpath()

getopt()

getpass()

getwd()

di queste non esistono versioni standard sicure

librerie dinamiche

- il link con librerie dinamiche può essere una vulnerabilità
  - alcuni sistemi permettono di sostituire le librerie dinamiche
  - comandi privilegiati possono linkare librerie scelte
- linux
  - permette di customizzare il path di ricerca
  - LD_LIBRARY_PATH
  - ma non permette customizzazione per programmi privilegiati (suid, guid)
- fino
  - cerca nella directory corrente le .dll e poi nelle directory di sistema - http://www.securityfocus.com/bid/1699/
- da Windws
  - safe dll search mode, Windows store apps

Defend your code:10 security tips (MSDN magazine)

1. Trust User Input at Your Own Peril
2. Protect Against Buffer Overruns
3. Prevent Cross-site Scripting
4. Don't Require sa Permissions
5. Watch that Crypto Code!
6. Reduce Your Attack Profile
7. Employ the Principle of Least Privilege
8. Pay Attention to Failure Modes
9. Impersonation is Fragile
10. Write Apps that Non-admins Can Actually Use

riferimenti

David A. Wheeler, “Secure Programming for Linux and Unix HOWTO -- Creating

http://www.dwheeler.com/secure-programs/

http://msdn.microsoft.com/