Software Security

Friday, March 23, 2018 1:14 PM

Secure programming

- Input handling
- Attacker can access resources, execute injected codes, crash
- Windows XP = 45 million source lines of codes

printf Vulnerability

- Second parameter not supplied, picked from call stack
  - `printf ("hello world %d");`
  - No checking for #param in program (reduced runtime efficiency)
- Allows attacker to obtain more information, crash (%s) or modify memory content (%n)
  - %s: pointer to memory, may not be able to access (privileges), leading to killed process and crash
  - %n: number of pointers printed out
  - Multiuser setting: elevated privilege -> system information obtained
  - Server-client setting: client can request for secret key

Preventive Measure

- printf(t)
  - For user-scanned input, have to check that there is no %d
- printf(f ,t)
  - Pass in user input as the second parameter
  - f is not user-supplied