Software Security 01

Cosa è la software security

Gianluca Amato
Università di Chieti-Pescara

https://cybersecnatlab.it

License & Disclaimer

License Information

Disclaimer

- We disclaim any warranties or representations as to the accuracy or completeness of this material.
- Materials are provided “as is” without warranty of any kind, either express or implied, including without limitation, warranties of merchantability, fitness for a particular purpose, and non-infringement.
- Under no circumstances shall we be liable for any loss, damage, liability or expense incurred or suffered which is claimed to have resulted from use of this material.

Cosa si intende per software security (1)

È la disciplina che si occupa di

- progettare
- sviluppare
- mantenere il software

in modo da

- prevenire vulnerabilità
- proteggere il sistema da attacchi malevoli

Cosa si intende per software security (2)

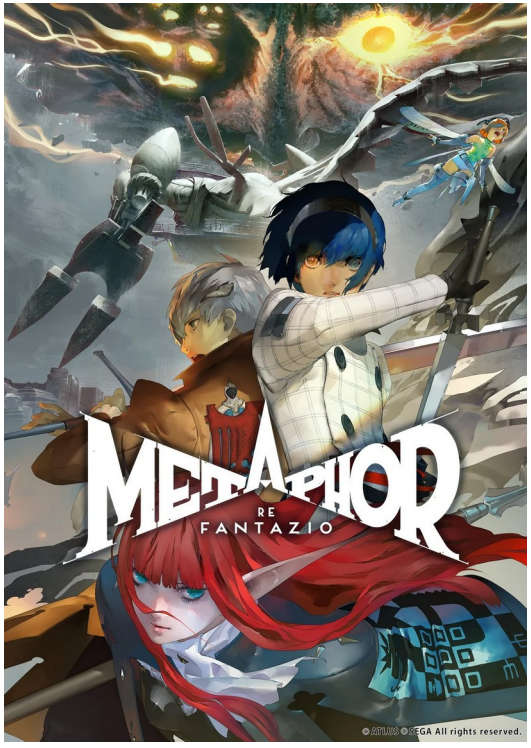
- Una delle aree più antiche della sicurezza informatica:
  - … quando Internet e i personal computer non esistevano ancora, la sicurezza software era già un problema rilevante.
- Ha alcune sotto-aree che avete già visto a lezione:
  - Web security

Scenario di software security: attacco locale

- L'attaccante:
  - ha a disposizione un programma;
  - può eseguire il programma nel proprio PC;
  - può quindi modificare il programma che viene effettivamente eseguito.
- L'attaccante vuole:
  - eseguire il programma, sebbene non abbia una licenza;
  - estrarre password o altri segreti dal programma;
  - modificare il funzionamento normale del programma
    - Esempio: cheat nei videogiochi

Esempio di attacco locale

- Metaphor: ReFantazio
  - È un videogioco della categoria J-RPG uscito a fine 2024;
  - la demo conteneva il gioco intero ma inaccessibile;
  - dopo poco tempo si trovava su Internet il *crack* per PC per rendere accessibile tutto il gioco.

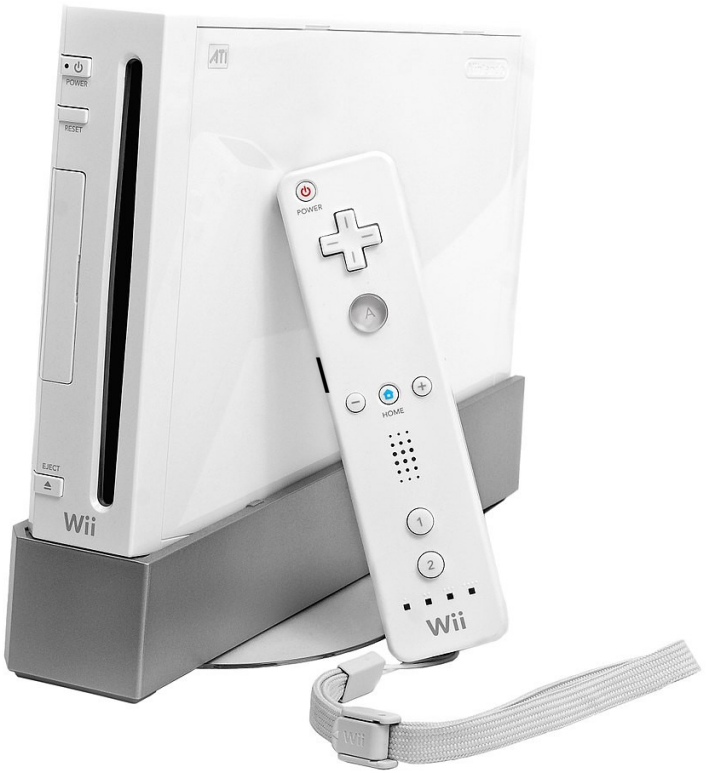


Scenario di software security: attacco remoto

- L'attaccante:
  - deve attaccare un programma in esecuzione in un computer su cui non ha un accesso diretto;
  - non può quindi modificare il programma in esecuzione;
  - potrebbe avere a disposizione il codice del programma per analizzarne le vulnerabilità.
- L'attaccante vuole:
  - eseguire funzioni non previste dal programma;
  - guadagnare un accesso diretto al sistema.

Esempio di attacco remoto (1)

- Nintendo Wii
  - Una delle console più craccate di sempre
  - Crack completamente via software
  - Causa di varie vulnerabilità <u>software</u> e <u>crittografiche</u> combinate



Esempio di attacco remoto (2)

- Equifax
  - una delle più grandi agenzie di credito negli USA, hackerata nel 2017;
  - gli aggressori hanno rubato i dati personali di oltre 147 milioni di persone;
  - i criminali hanno sfruttato una vulnerabilità nota in Apache Struts, un framework open-source usato per le applicazioni web Java
  - la vulnerabilità era un Remote Code Execution (RCE): permetteva agli attaccanti di eseguire comandi arbitrari sul server.
  - https://en.wikipedia.org/wiki/2017_Equifax_data_breach

Prerequisiti

- I prerequisiti per queste lezioni (irrealistici...)
  - Conoscenza del linguaggio C:
    - Conoscenza di base
    - Puntatori
  - Conoscenza del linguaggio assembly Intel x86 e x86-64
    - Conoscenze di base
    - Conoscenza di come il codice C viene tradotto in linguaggio assembly
  - Conoscenza di base del linguaggio Python

Software Security 01

Cosa è la software security

FINE

Gianluca Amato
Università di Chieti-Pescara

CYBER CHALLENGE.IT

CYBERSECURITY NATIONAL LABORATORY

https://cybersecnatlab.it