**SOFTWARE SECURITY**

1. **Lines of code ( LOC )**
2. **Bugs in lines of code**

Để fix lỗi thì tốn rất nhiều thời gian, nhưng phần mềm và cơ sở dữ liệu ngày càng lớn 🡪 khó fix, tốn nhiều thời gian, chi phí.

1. **Cost of fixing bugs**

Tốn nhiều thời gian và công sức, chi phí

Có các giai đoạn : có 5 giai đoạn, càng về giai đoạn sau code càng phức tạp nên chi phí fix ngày càng cao.

1. **Program security flaws**
2. **Software security issues**

* Insecure interaction between components : Giao tiếp, sử dụng từ xa, qua mạng 🡪 dễ bị mất thông tin do trung gian internet có nhiều rủi ro.
* Risky resource management
* Leaky defenses

Lỗi hay xảy ra nhất là buffer overflow ( 37% )

1. Defensive programming

Đảm bảo code và chương trình không bị lỗi, giảm thiểu lỗi.

1. Secure software
2. Security in software development life cycle

Requirements 🡪 design 🡪 code 🡪 testing 🡪 release 🡪 feedback

1. Bảo mật trong chu trình phát triển phần mềm
2. **Buffer overflows**

Software vulnnerabilitites

The buffer overflow problem

1. Program memory layout

Stack : store local biến in hàm . store data related to function calls.

Heap :

BSS segment :

Data segment:

Text

Stack 🡪 🡨 Heap BSS segment Data segment Text segment

Khi nào đi ra khỏi stack ?

Khi hàm đó được thực hiện xong.

Khi làm xong hàm main được đưa vào stacck

1. A Stack Frame ( con trỏ khung )

Ex : layout for a stack fale

1. Buffer overflow basic

Stack overflow

1. Stack smash – overwriting the saved epi