

Ministero della Salute
Educazione Continua in Medicina

Sicurezza informatica

Emilio Pavia

Introduzione

Qualsiasi sistema informatico presenta delle debolezze teoriche e reali.

Introduzione

Qualsiasi sistema informatico presenta delle debolezze teoriche e reali.

Lo scopo della sicurezza informatica è escogitare modi per impedire che le debolezze vengano sfruttate.

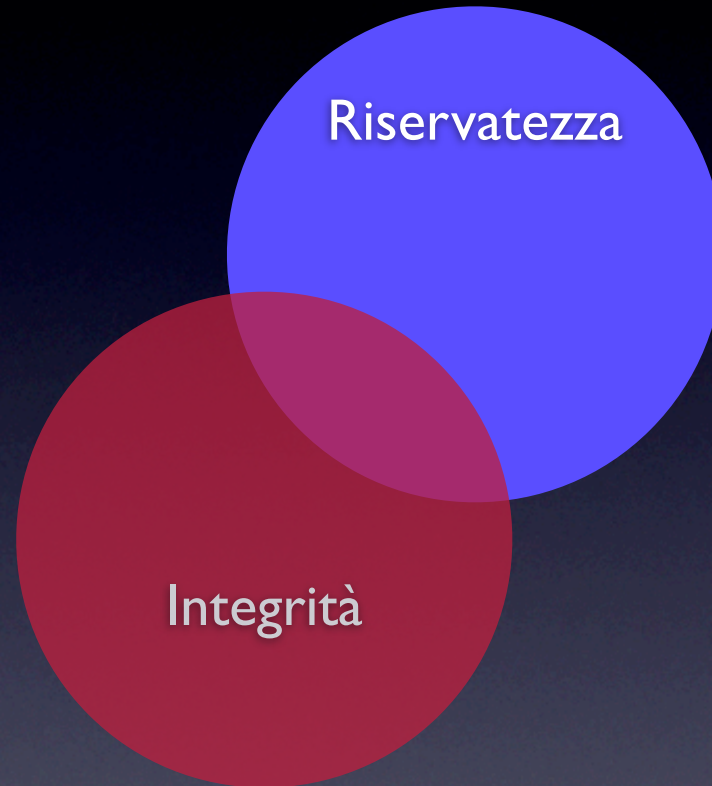
Obiettivi

Obiettivi



Riservatezza

Obiettivi



Obiettivi



Sicurezza dei programmi

Un programma è insicuro se produce comportamenti diversi da quelli per cui è stato progettato.

Errori nei programmi

- Errori non intenzionali

Errori nei programmi

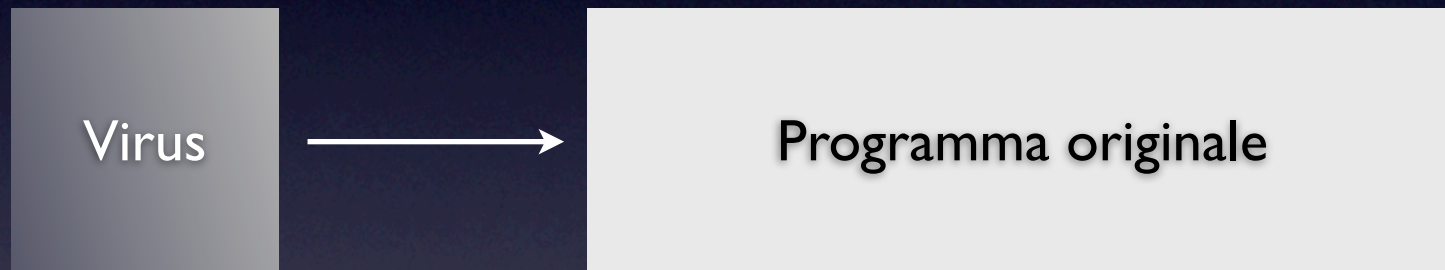
- Errori non intenzionali
- Errori intenzionali (codice maligno)

Tassonomia

- Virus
- Cavallo di Troia
- Bomba logica o a tempo
- Backdoor
- Worm
- Coniglio

Virus

Si unisce a un programma e propaga copie di sé stesso in altri programmi.



Virus

Si unisce a un programma e propaga copie di sé stesso in altri programmi.



Virus

The diagram consists of a horizontal rectangle divided into two sections. The left section is a smaller, darker gray rectangle containing the word 'Virus'. The right section is a larger, lighter gray rectangle containing the words 'Programma originale'. This visualizes the concept of a virus attaching to a host program.

Programma originale

Cavallo di Troia

Codice maligno che oltre al suo effetto primario, presenta un secondo effetto maligno non ovvio.

Bomba logica o a tempo

Innesca un'azione al verificarsi di un'azione o allo scoccare di un istante specificato.

Backdoor

Codice maligno che consente l'accesso non autorizzato alle funzionalità di un programma o del sistema.

Worm

Programma che diffonde copie di sé stesso attraverso una rete. La differenza tra worm e virus è che i worm si diffondono solo sulle reti, mentre i virus sfruttano qualsiasi supporto.

Coniglio

Codice maligno che ha come obiettivo quello di replicarsi senza limiti allo scopo di esaurire le risorse.

Strumenti di protezione

Strumenti di protezione

I. Non usate Microsoft Windows!

Strumenti di protezione

2. Se proprio dovete, dotatevi di un buon antivirus (buono non è sinonimo di costoso o famoso)

Strumenti di protezione

2. Se proprio dovete, dotatevi di un buon antivirus (buono non è sinonimo di costoso o famoso)

IMPORTANTE: aggiornare l'antivirus quotidianamente!

Strumenti di protezione

2. Se proprio dovete, dotatevi di un buon antivirus (buono non è sinonimo di costoso o famoso)

IMPORTANTE: aggiornare l'antivirus quotidianamente!

Avere un antivirus non aggiornato è peggio che non averne!

Strumenti di protezione

3. Usare tanto buonsenso...

Le insidie della Rete

- Spam (???)
- Spyware
- Dialer
- Phishing
- Spoofing

Mai fidarsi!