Software Security

Abner Ballardo Urco
a.k.a.
MoDuLe LoSt

The Trinity of Trouble

- Complejidad
  - LOC = Lineas de código
  - A más líneas,... MÁS BUGS!
- Extensibilidad
  - Permite ejecutar código malicioso
- Conectividad
  - Pequeñas fallas pueden propagarse y causar problemas más grandes

Application Security

- Establece políticas de seguridad:
  - Qué se puede ejecutar
  - Cómo puede cambiar cierto recurso
  - Que puede hacer el software que se está ejecutando

Software Security

- Se interesa en:
  - Diseñar software que sea seguro
  - Asegurarse que el software sea seguro
  - Educar a los desarrolladores, arquitectos, y usuarios

Taxonomía

- **Bug:** Es un problema en el software, un problema simple de implementación.
- **Flaw:** Es instanciado por el código ejecutable de un software. Puede estar presente o no en el diseño del software.
- **Vulnerabilities:** Bugs + Flaws

Sobre Seguridad

- No existe un solución total en Software Security.
- Existen herramientas que analizan código pero no pueden reemplazar la experiencia o encontrar vulnerabilidades.

Sobre Seguridad

- En los 90's se inició el boom de productos de seguridad: firewalls, antivirus, criptografía. Sin embargo las vulnerabilidades se han incrementado

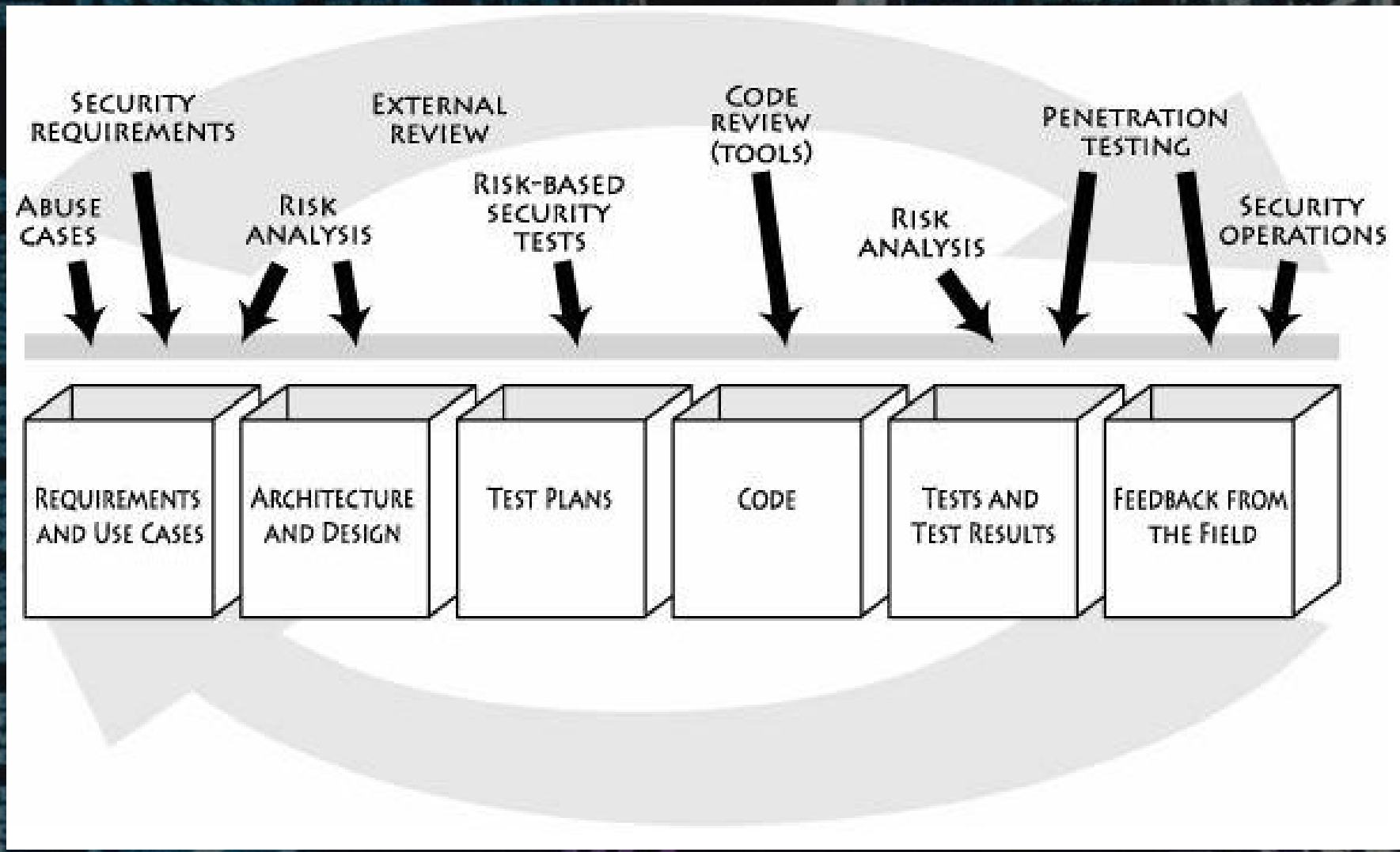
Año	Vulnerabilidades
1995	171
1996	345
1997	331
1998	322
1999	417
2000	1090
2001	2433
2002	4129
2003	3784
2004	3780
2005	5990
2006	8064

CERT/CC

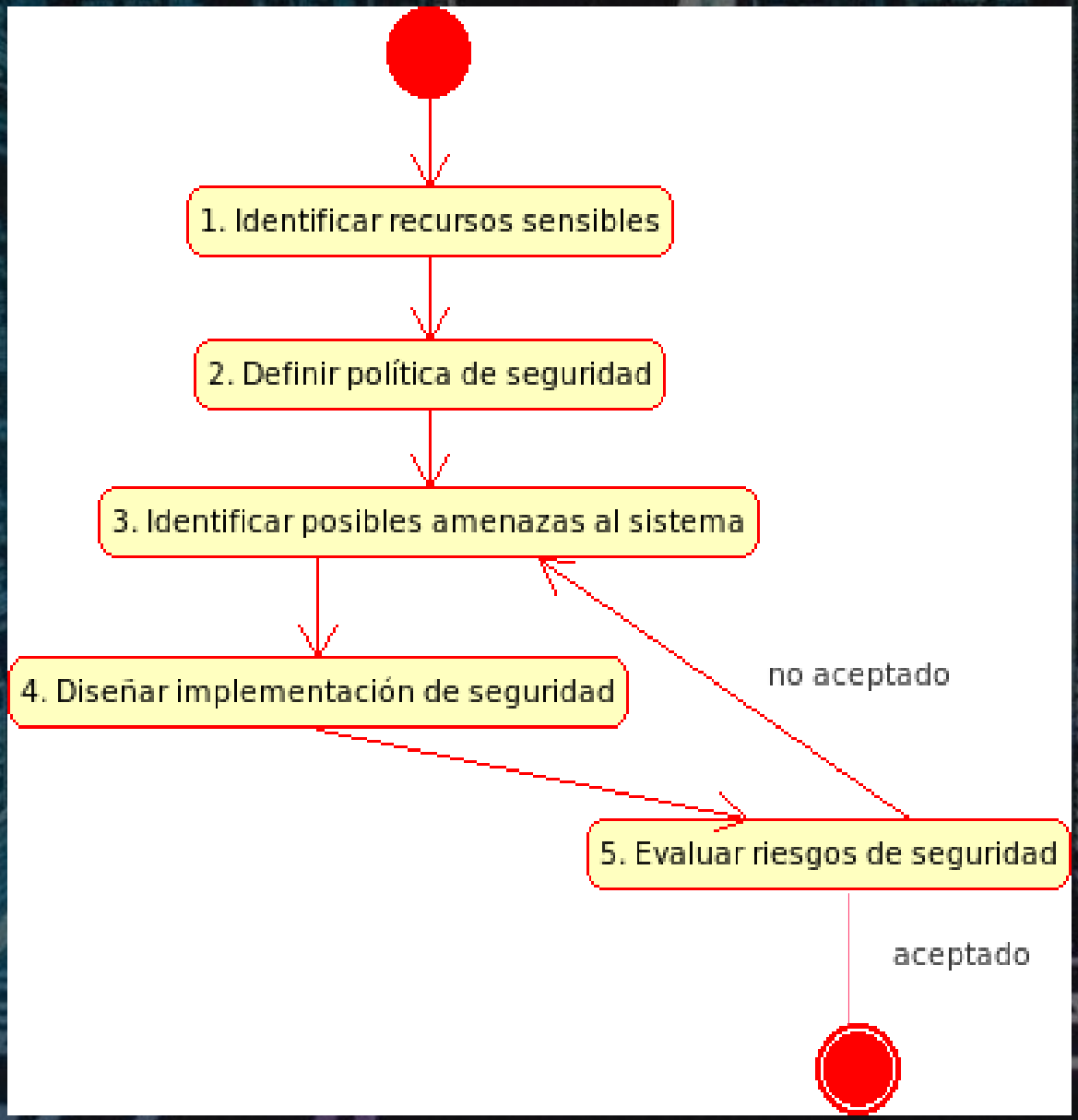
Sobre Seguridad

- Los firewalls hacen muy poco por proteger redes.
- Productos de detección de intrusos son suceptibles a errores y pueden causar falsas alarmas.
- El problema está en que seguridad es visto como un producto!

Desarrollo de software



Desarrollo de software



PHP - 2007/03/20

- Problem:
  - PHP hash_update_file() Already Freed Resource Access Vulnerability
- Description:
  - A malicious user stream can trick the hash_update_file() function into accessing an already freed hash resource. This can lead to arbitrary code execution.
- Version:
  - Affected is PHP 5 <= 5.2.1

MySQL – 2007/03/09

- Problem:
  - MySQL Single Row SubSelect Remote Denial Of Service Vulnerability
- Description:
  - An attacker can exploit this issue to crash the application, denying access to legitimate users. The attacker may also be able to execute arbitrary code, but this has not yet been confirmed.
- Version:
  - Prior to 5.0.36

Wordpress - 2007/02/26

- Problem:
  - PHP Cross-Site Scripting Vulnerability
- Description:
  - Wordpress is prone to a cross-site scripting vulnerability because the application fails to properly sanitize user-supplied input.
- Version:
  - Wordpress 2.1.1; other versions may also be affected

Abner Ballardo Urco
a.k.a.
MoDuLe LoSt

Email: modlost@modlost.net
Website: http://www.modlost.net/
Podcast: http://radio.modlost.net/
Planet: http://www.openperuplanet.org/
Community: http://www.opensourcespot.org/