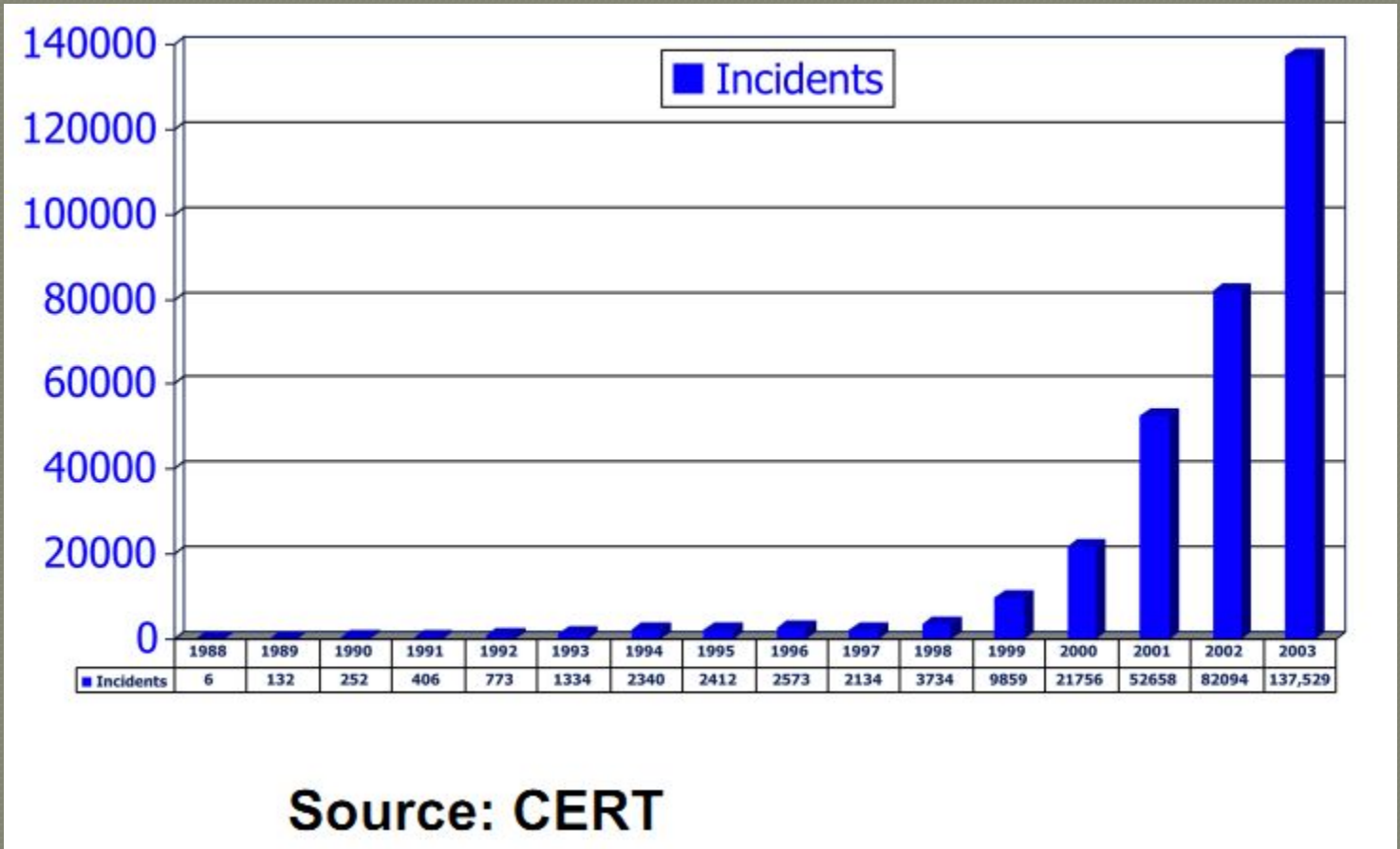
Софтверски сигурностни пропусти – детекција и превенција

Даме Јованоски

Предизвици

- Pwn2own – Предизвик за пронаоѓање на пропусти во пребарувачите(IE,Mozzila Firefox и Google Chrome)
  Награда:$100,000.
- Hex-Rays –пронаоѓање на сигурностни пропусти во нивните продукти
  Награда: $3000.
- Google предизвик за наоѓање на сигурностни пропусти во Chrome
  Награда:$20,000.

Факти



	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002	2003
Incidents	6	132	252	406	773	1334	2340	2412	2573	2134	3734	9859	21756	52658	82094	137,529

Source: CERT

IEEE Computer Magazine

As software dependence reaches critical levels, threats become more pervasive, and losses become more costly, higher education must place more value on the tenets of software assurance. Courses must focus not only on security but on providing justified confidence in the software or system throughout its life cycle.

A moving-target defense enables controlled movements across multiple system dimensions to reduce the window of opportunity for attackers to exploit system vulnerabilities.

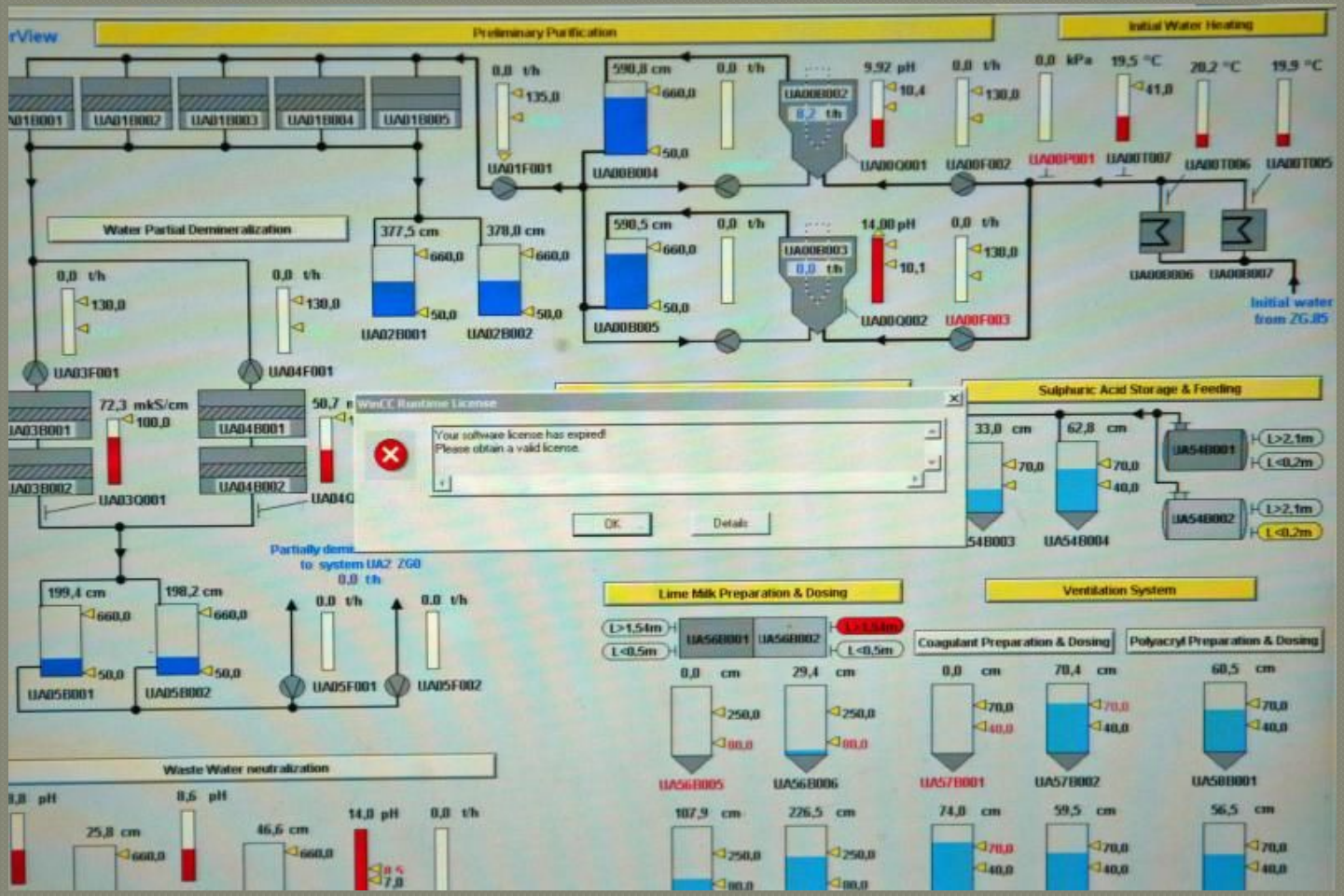
Cyberattacks continue to grow in number and sophistication, as the following trends show:[4]

- organized nation-state attacks against the Pentagon and other facilities in the US;
- organized nation-state attacks on Estonia and Georgia;
- rising identity theft via the Internet;
- undocumented features in open source applications code that cause software life-cycle problems;
- open source flaws, typically on the order of 1 per 103 lines of code;
- use of botnets and other organized Internet exploits;
- website and Web application exploits; and
- compromising unsecured data.

Geekonomics: The Real Cost of Insecure Software

- The Real Cost of Insecure Software
- • In 1996, software defects in a Boeing 757 caused a crash that killed 70 people…
- • In 2003, a software vulnerability helped cause the largest U.S. power outage in decades…
- • In 2004, known software weaknesses let a hacker invade T-Mobile, capturing everything from passwords to Paris Hilton's photos…
- • In 2005, 23,900 Toyota Priuses were recalled for software errors that could cause the cars to shut down at highway speeds…
- • In 2006 dubbed "The Year of Cybercrime," 7,000 software vulnerabilities were discovered that hackers could use to access private information…
- • In 2007, operatives in two nations brazenly exploited software vulnerabilities to cripple the infrastructure and steal trade secrets from other sovereign nations…

(цел на напад – SCADA системи)

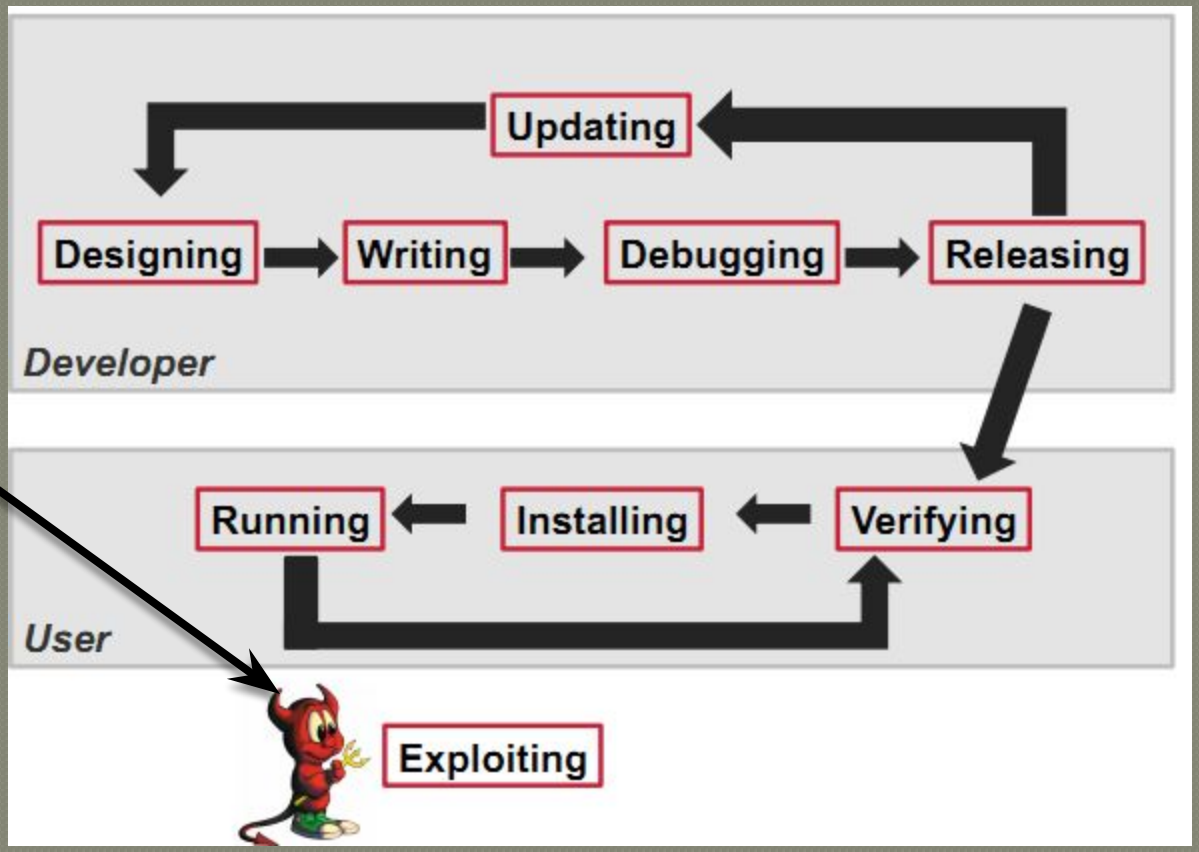


Срцето на Stuxnet црвот

Characteristics	MS10-002	MS10-046	MS10-061	0-day (unpatched)
Vulnerable versions	all versions of MS Internet Explorer (6, 7, 8)	all versions of MS Windows (WinXP, Vista, 7, …)	all versions of MS Windows (WinXP, Vista, 7, …)	WinXP and Win2000
Layered shellcode	yes	no	no	yes
Remote attacks	yes	yes	yes (only for WinXP)	no
Other vectors	no	yes	yes	no

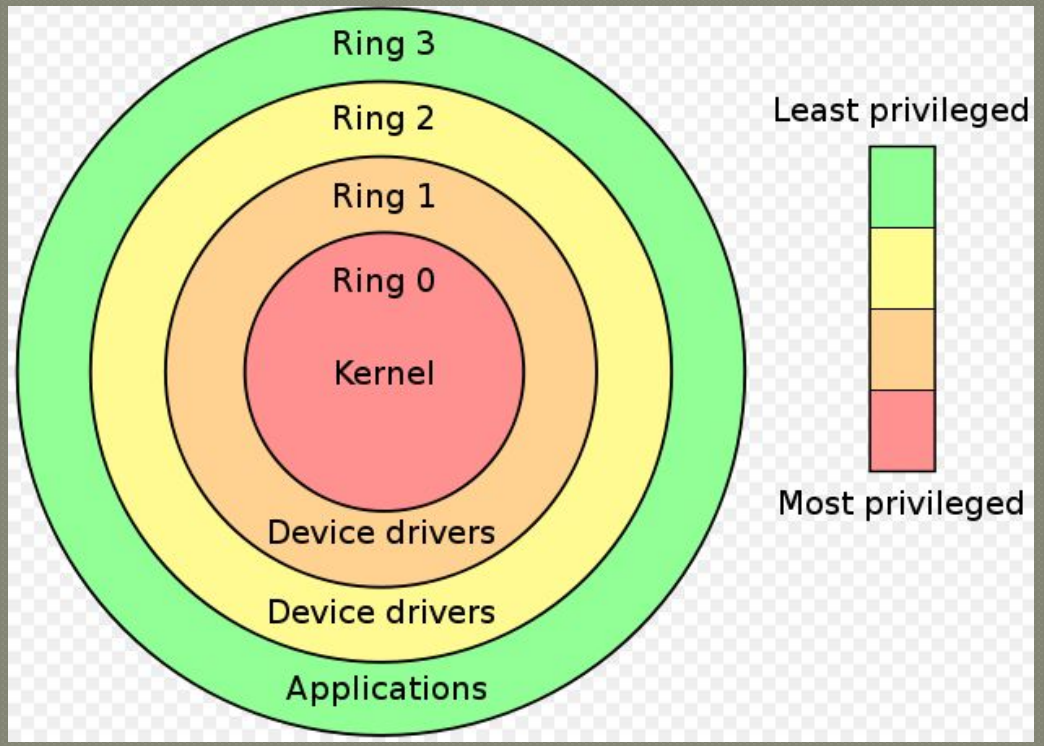
Циклус на развој на програми кои ги користат софтверските пропусти

Процес или циклус на развој на програми кои ги искористуваат софтверските сигурностни пропусти



Целта на напѓачот

- Напаѓачот има за цел да пристапи до системот којшто го напаѓа ескалирање за придобивање на привилегии т.е ring0.



Најчести и најпознати видови на софтверски сигурностни пропусти

- Buffer overflow
- String overflow
- Integer overflow
- Heap overflow

- Листа на останати видови на сигурностни пропусти: http://www.owasp.org/index.php/Category:Vulnerability

Дебагери

- Microsoft Windows платформа:
  - OllyDbg
  - Immunity Debugger
  - WinDbg

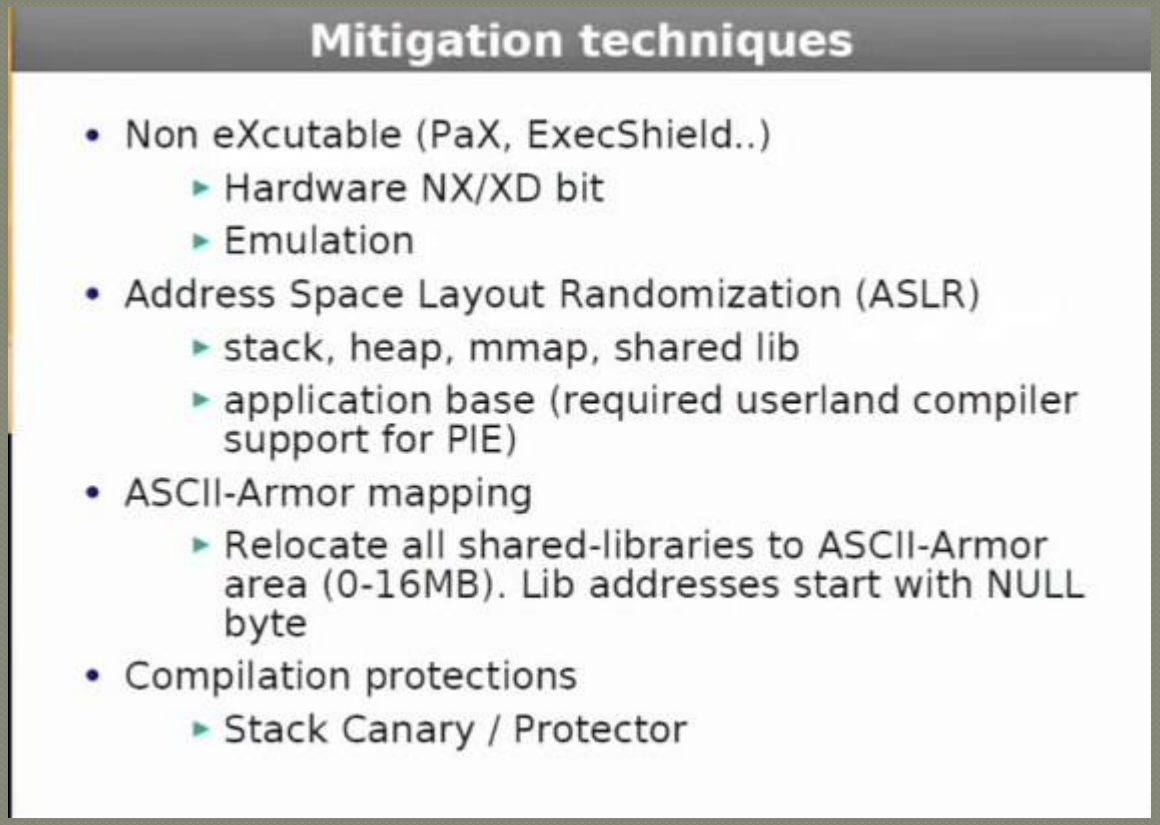
- Linux платформа:
  - gdb
  - edb

Безбедностни механизми (Microsoft Windows)

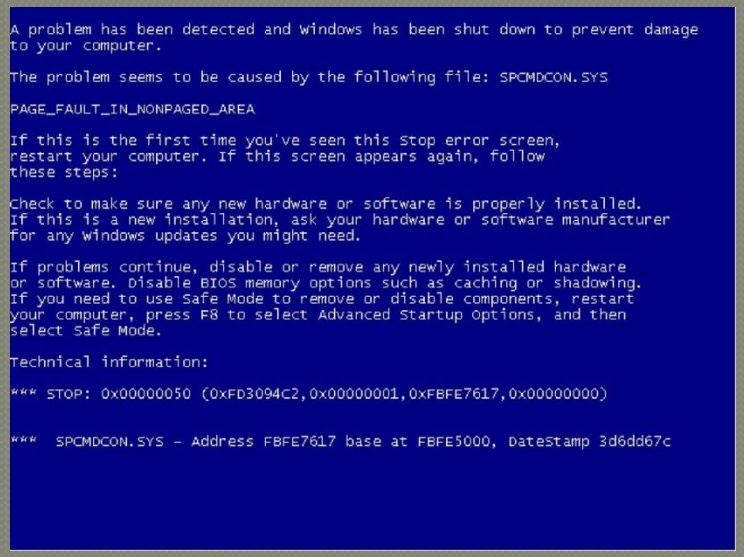
OS evolution

	XP SP2, SP3	2003 SP1, SP2	Vista SP0	Vista SP1	2008 SP0
GS					
stack cookies	yes	yes	yes	yes	yes
variable reordering	yes	yes	yes	yes	yes
#pragma strict_gs_check	no	no	no	?	?
SafeSEH					
SEH handler validation	yes	yes	yes	yes	yes
SEH chain validation	no	no	no	yes [1]	yes
Heap protection					
safe unlinking	yes	yes	yes	yes	yes
safe lookaside lists	no	no	yes	yes	yes
heap metadata cookies	yes	yes	yes	yes	yes
heap metadata encryption	no	no	yes	yes	yes
DEP					
NX support	yes	yes	yes	yes	yes
permanent DEP	no	no	no	yes	yes
OptOut mode by default	no	yes	no	no	yes
ASLR					
PEB, TEB	yes	yes	yes	yes	yes
heap	no	no	yes	yes	yes
stack	no	no	yes	yes	yes
images	no	no	yes	yes	yes

Безбедностни механизми (Microsoft Windows)



Резултат на искористување на ранливост



Th3 3nd