

# Софтверски сигурносни пропусти – детекција и превенција

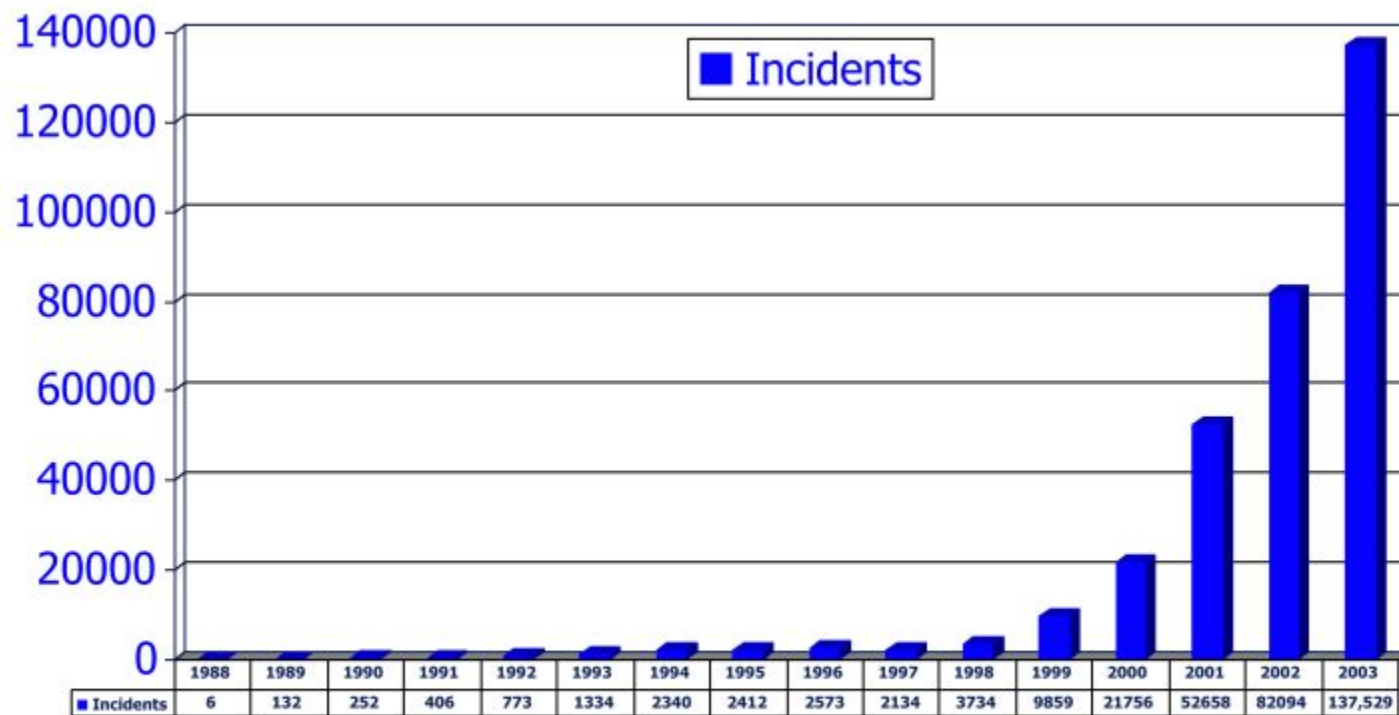
Даме Јованоски

# Предизвици

---

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

# Факти



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:<sup>4</sup>

- 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 10<sup>3</sup> lines of code;
- use of botnets and other organized Internet exploits;
- website and Web application exploits; and
- compromising unsecured data.

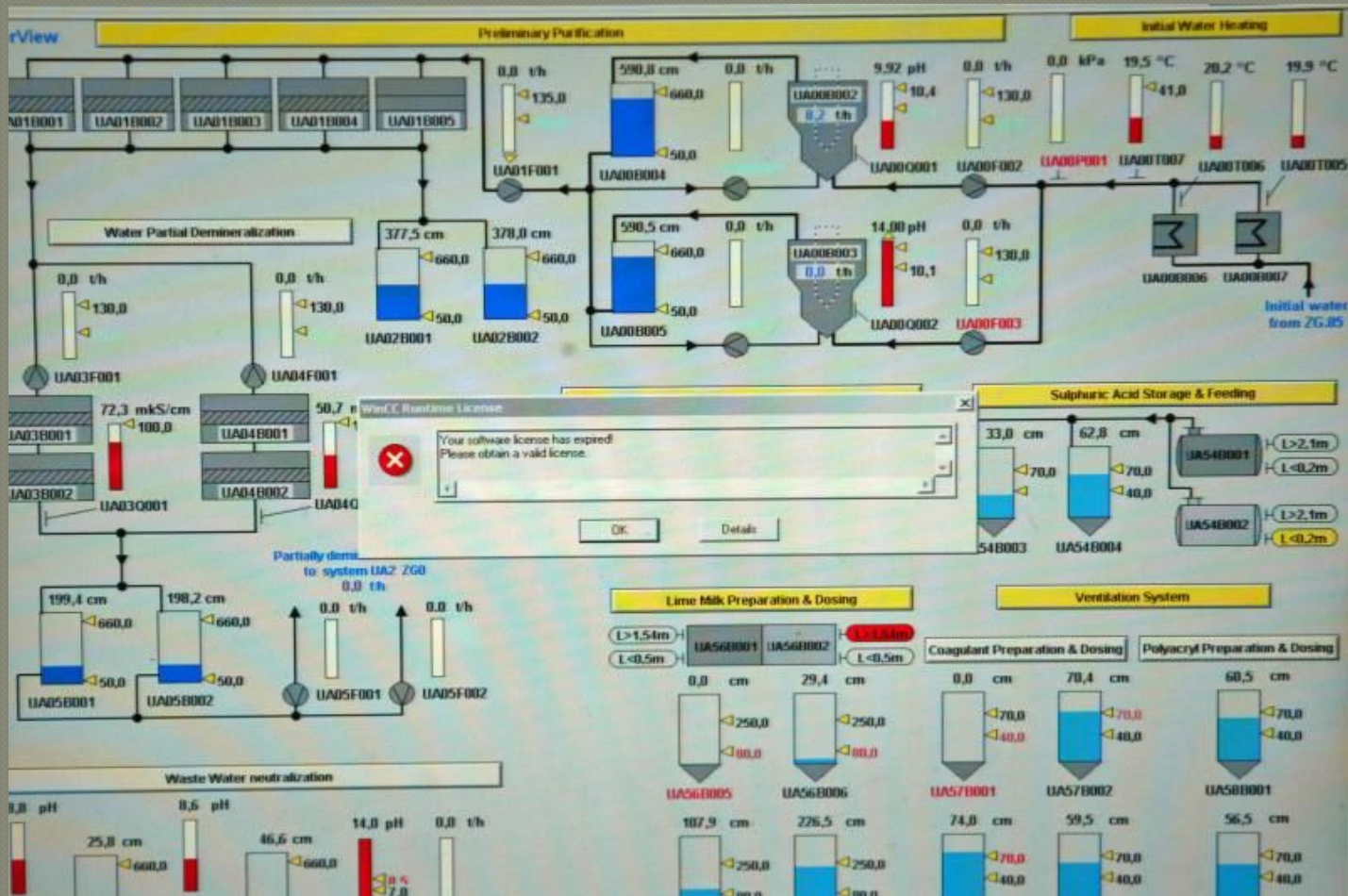
# Geekonomics: The Real Cost of Insecure Software

---

- 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)

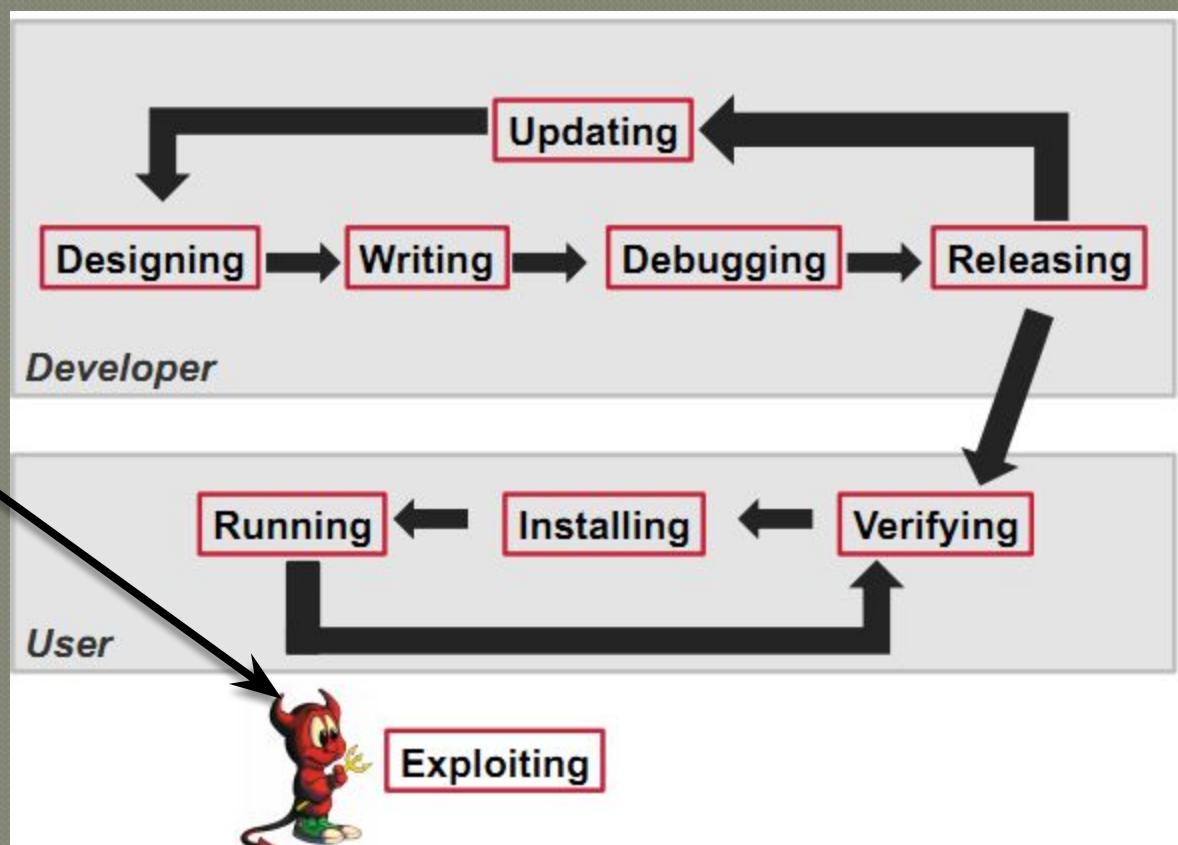


# Срцето на Stuxnet црвот

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

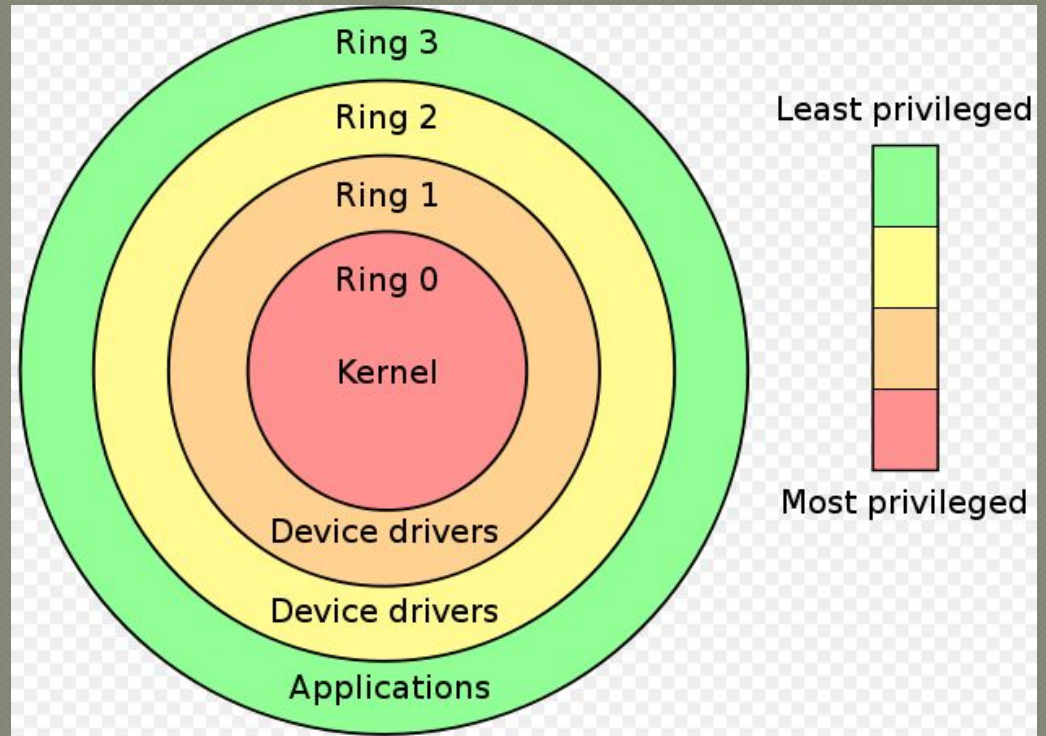
Процес или  
циклус на развој  
на програми кои  
ги искористуваат  
софтверските  
сигурностни  
пропусти





# Целта на напаѓачот

- 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 сигурносни пропусти

---

- Buffer overflow
- String overflow
- Integer overflow
- Heap overflow
  
- Листа на останати видови на сигурносни пропусти:  
<http://www.owasp.org/index.php/Category:Vulnerability>

# Дебагери

---

- Microsoft Windows платформа:

- ▢ OllyDbg
- ▢ Immunity Debugger
- ▢ WinDbg

- Linux платформа:

- ▢ gdb
- ▢ edb

# Безбедносни механизми (Microsoft Windows)

## OS evolution

	XP SP2, SP3	2003 SP1, SP2	Vista SP0	Vista SP1	2008 SP0
<b>GS</b>					
stack cookies	yes	yes	yes	yes	yes
variable reordering	yes	yes	yes	yes	yes
#pragma strict_gs_check	no	no	no	?	?
<b>SafeSEH</b>					
SEH handler validation	yes	yes	yes	yes	yes
SEH chain validation	no	no	no	yes <sup>1</sup>	yes
<b>Heap protection</b>					
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
<b>DEP</b>					
NX support	yes	yes	yes	yes	yes
permanent DEP	no	no	no	yes	yes
OptOut mode by default	no	yes	no	no	yes
<b>ASLR</b>					
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

# Безбедносни механизми (Microsoft Windows)

## Mitigation techniques

- Non eXcutable (PaX, ExecShield..)
  - ▶ Hardware NX/XD bit
  - ▶ Emulation
- Address Space Layout Randomization (ASLR)
  - ▶ stack, heap, mmap, shared lib
  - ▶ application base (required userland compiler support for PIE)
- ASCII-Armor mapping
  - ▶ Relocate all shared-libraries to ASCII-Armor area (0-16MB). Lib addresses start with NULL byte
- Compilation protections
  - ▶ Stack Canary / Protector



# Резултат на искористување на ранливост

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c
```

## Internet Explorer

**You chose to end the nonresponsive program, Internet Explorer.**

The program is not responding.

### **Please tell Microsoft about this problem.**

We have created an error report that you can send to help us improve Internet Explorer. We will treat this report as confidential and anonymous.

To see what data this error report contains, [click here](#).

# Th3 3nd

---



**BUFFER OVERFLOW  
ATTACK**