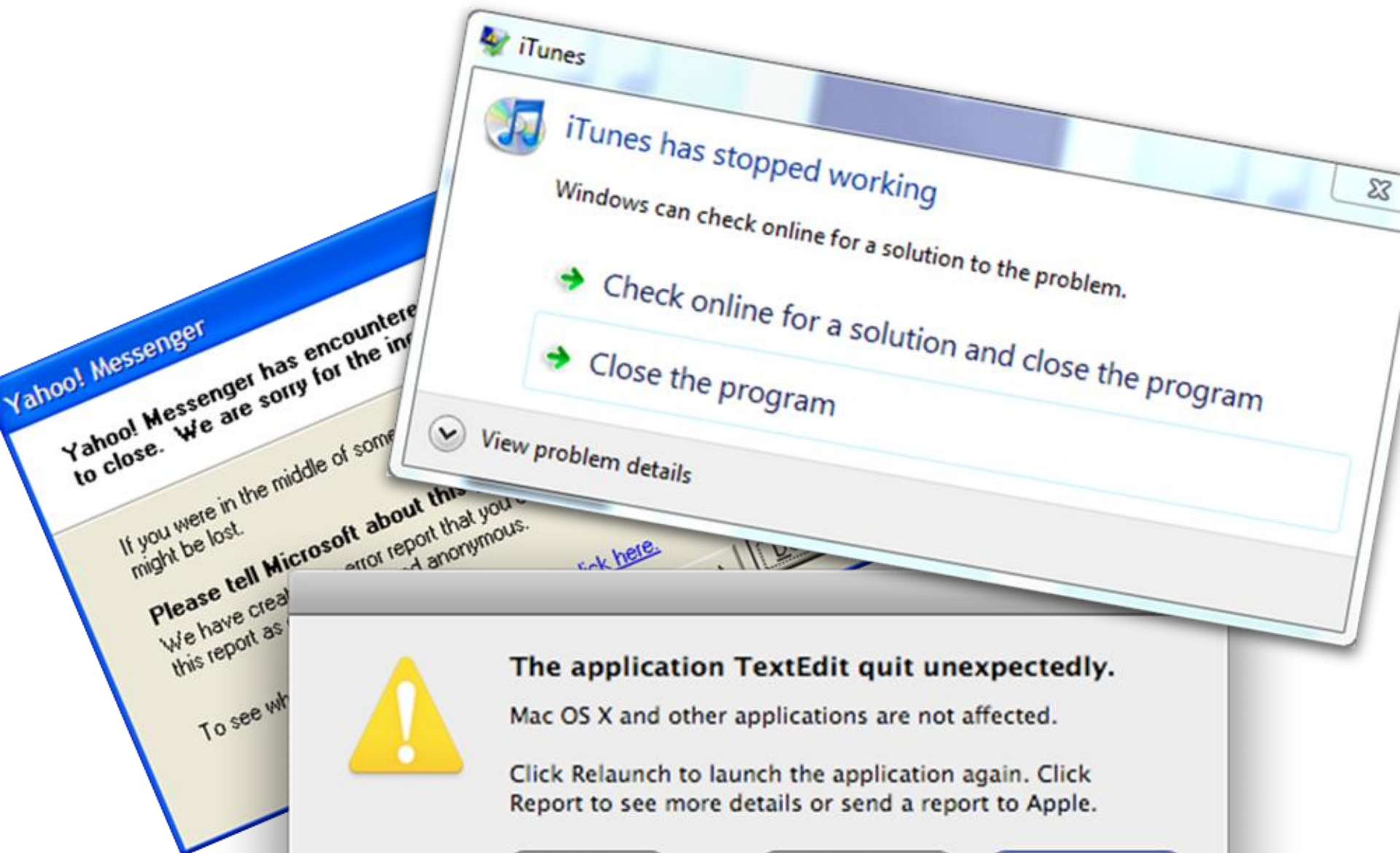




PLAYING IN THE SANDBOX

David Benjamin

Process Isolation in Google Chrome



The application TextEdit quit unexpectedly.

Mac OS X and other applications are not affected.

Click Relaunch to launch the application again. Click Report to see more details or send a report to Apple.

Ignore

Report...

Relaunch

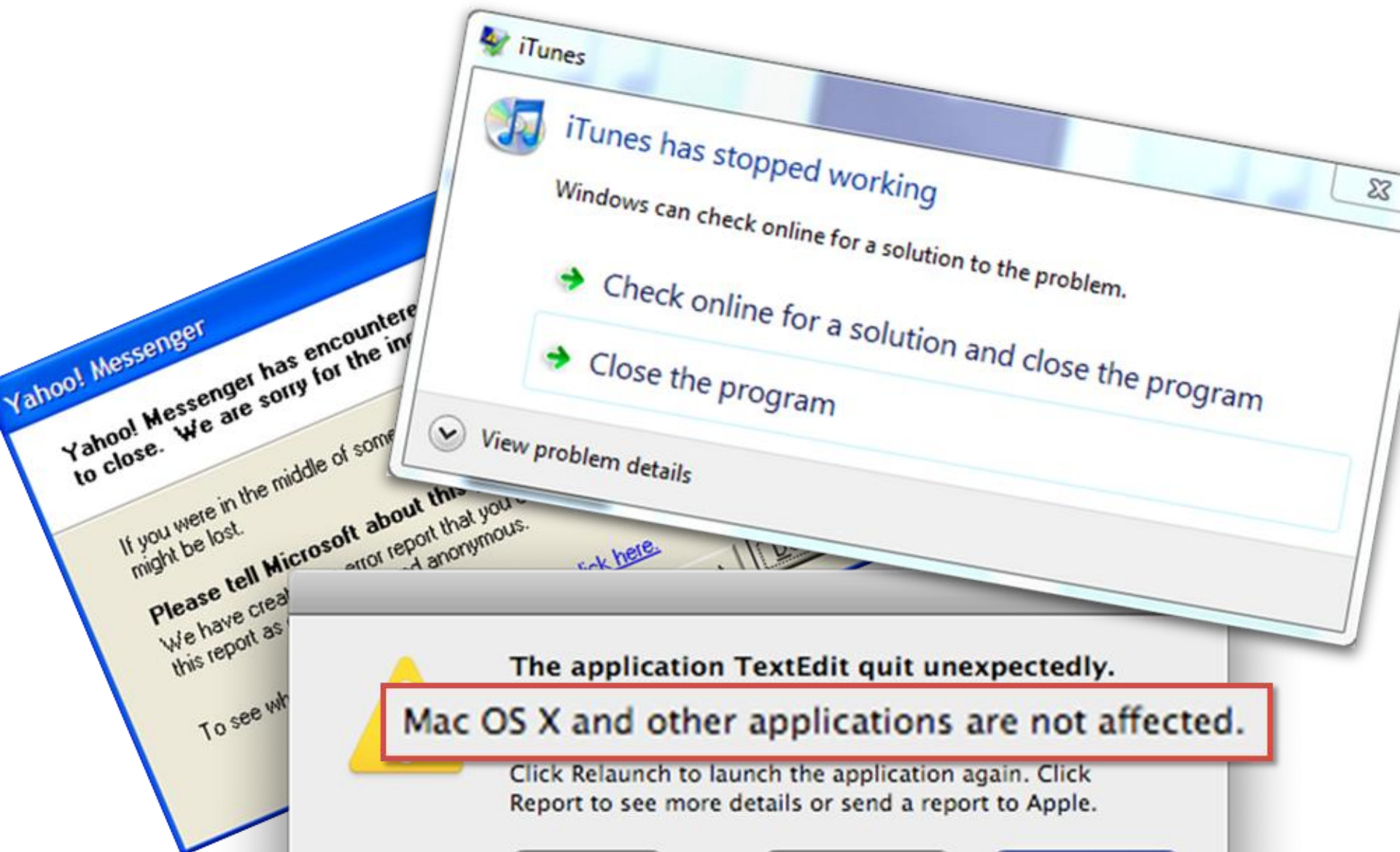
*** STOP: 0x00000019 (0x00000000,0xC00E0FF0,0xFFFFEFD4,0xC0000000)
BAD_POOL_HEADER

CPUID: GenuineIntel 5.2.c irq1:1f SYSVER 0xf0000565

Dll	Base	DateStmp	-	Name	Dll	Base	DateStmp	-	Name
80100000	3202c07e	-	ntoskrnl.exe	80010000	31ee6c52	-	hal.dll		
80001000	31ed06b4	-	atapi.sys	80006000	31ec6c74	-	SCSIPTORT.SYS		
802c6000	31ed06bf	-	aic78xx.sys	802cd000	31ed237c	-	Disk.sys		
802d1000	31ec6c7a	-	CLASS2.SYS	8037c000	31eed0a7	-	Ntfs.sys		
fc698000	31ec6c7d	-	Floppy.SYS	fc6a8000	31ec6ca1	-	Cdrom.SYS		
fc90a000	31ec6df7	-	Fs_Rec.SYS	fc9c9000	31ec6c99	-	Null.SYS		
fc864000	31ed868b	-	KSecDD.SYS	fc9ca000	31ec6c78	-	Beep.SYS		
fc6d8000	31ec6c90	-	i8042prt.sys	fc86c000	31ec6c97	-	mouclass.sys		
fc874000	31ec6c94	-	kbdclass.sys	fc6f0000	31f50722	-	VIDEOPTORT.SYS		
feffa000	31ec6c62	-	mga_mil.sys	fc890000	31ec6c6d	-	vga.sys		
fc708000	31ec6ccb	-	Msfs.SYS	fc4b0000	31ec6cc7	-	Npfs.SYS		
feefbc000	31eed262	-	NDIS.SYS	a0000000	31f954f7	-	win32k.sys		
feffa4000	31f91a51	-	mga.dll	fec31000	31eedd07	-	Fastfat.SYS		
feb8c000	31ec6e6c	-	TDI.SYS	feaf0000	31ed0754	-	nbf.sys		
feacf000	31f130a7	-	tcpip.sys	feab3000	31f50a65	-	netbt.sys		
fc550000	31601a30	-	el59x.sys	fc560000	31f8f864	-	afd.sys		
fc718000	31ec6e7a	-	nethbios.sys	fc858000	31ec6c9b	-	Parport.sys		
fc870000	31ec6c9b	-	Parallel.SYS	fc954000	31ec6c9d	-	ParVdm.SYS		
fc5b0000	31ec6cb1	-	Serial.SYS	fea4c000	31f5003b	-	rdr.sys		
fea3b000	31f7a1ba	-	mup.sys	fe9da000	32031abe	-	srv.sys		

Address	dword	dump	Build [1381]	-	Name		
fec32d84	80143e00	80143e00	80144000	ffdf0000	00070b02	-	KSecDD.SYS
801471c8	80144000	80144000	ffdf0000	c03000b0	00000001	-	ntoskrnl.exe
801471dc	80122000	f0003fe0	f030eee0	e133c4b4	e133cd40	-	ntoskrnl.exe
80147304	803023f0	0000023c	00000034	00000000	00000000	-	ntoskrnl.exe

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option.



Yahoo! Messenger

Yahoo! Messenger has encountered an error and needs to close. We are sorry for the inconvenience.

If you were in the middle of something, it might be lost.

Please tell Microsoft about this error report that you created. We have created this report as anonymous.

To see what

iTunes



iTunes has stopped working

Windows can check online for a solution to the problem.

- Check online for a solution and close the program
- Close the program



View problem details

The application TextEdit quit unexpectedly.

Mac OS X and other applications are not affected.

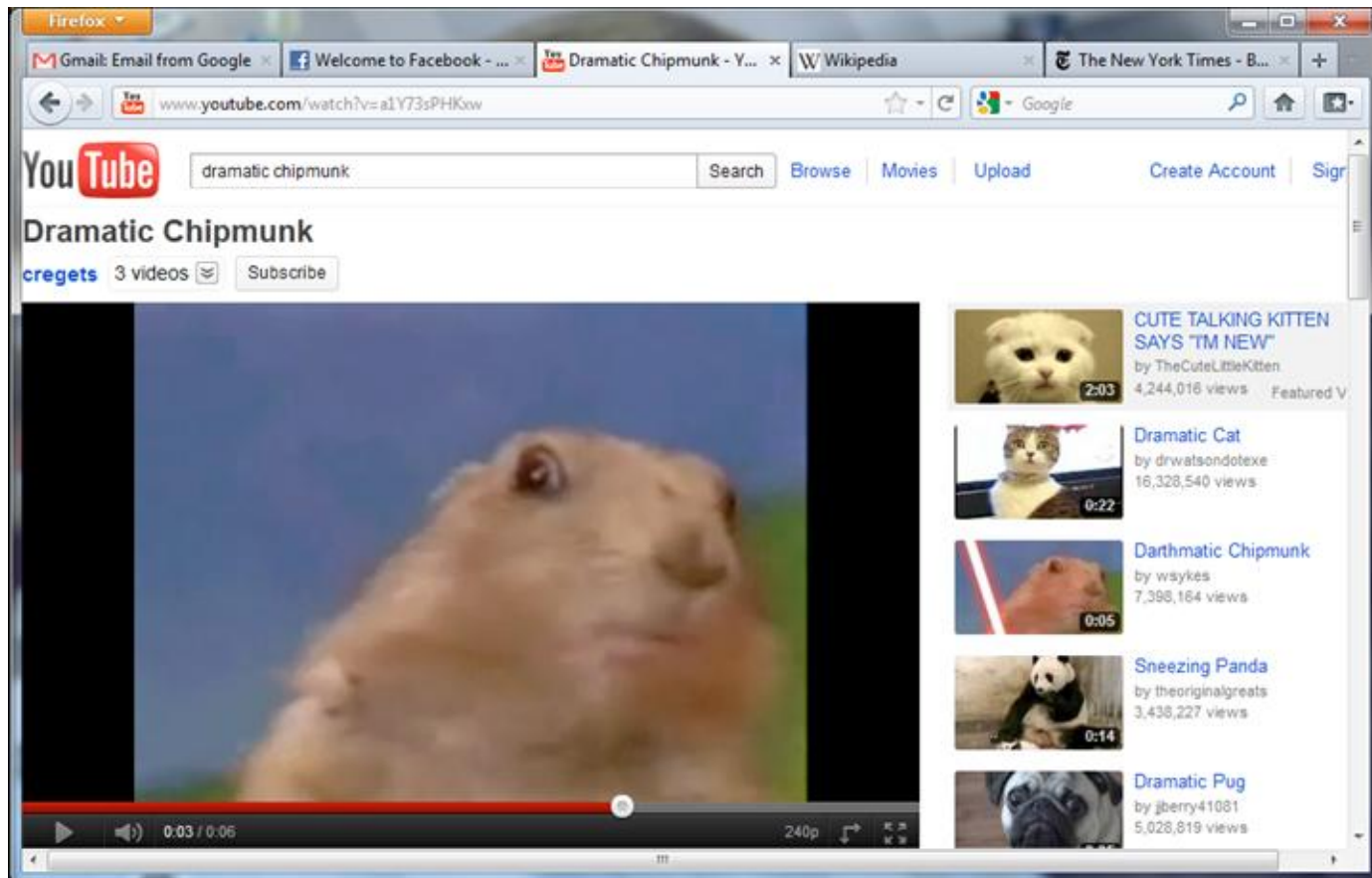
Click Relaunch to launch the application again. Click Report to see more details or send a report to Apple.

Ignore

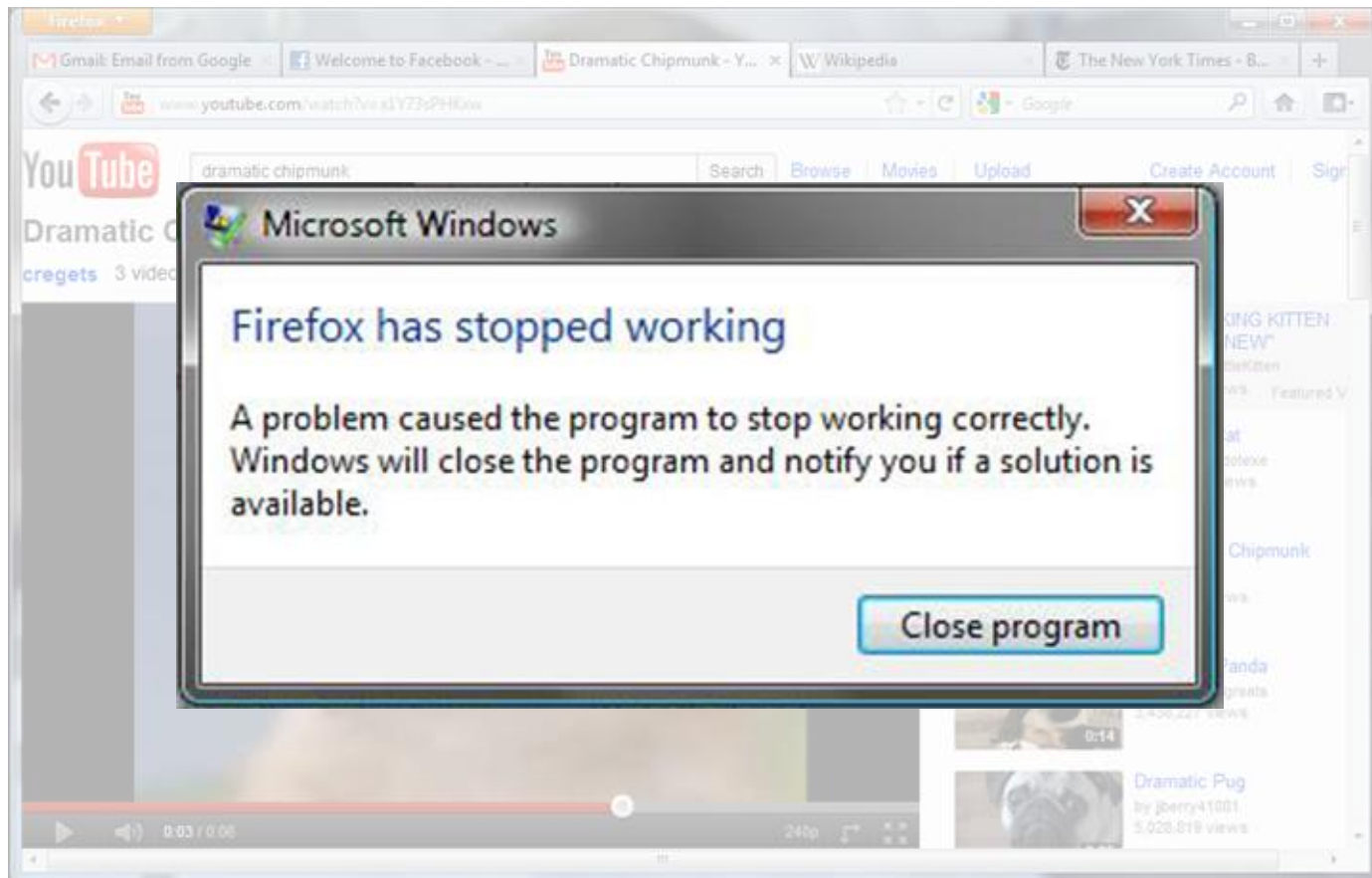
Report...

Relaunch

What if a webpage crashes?

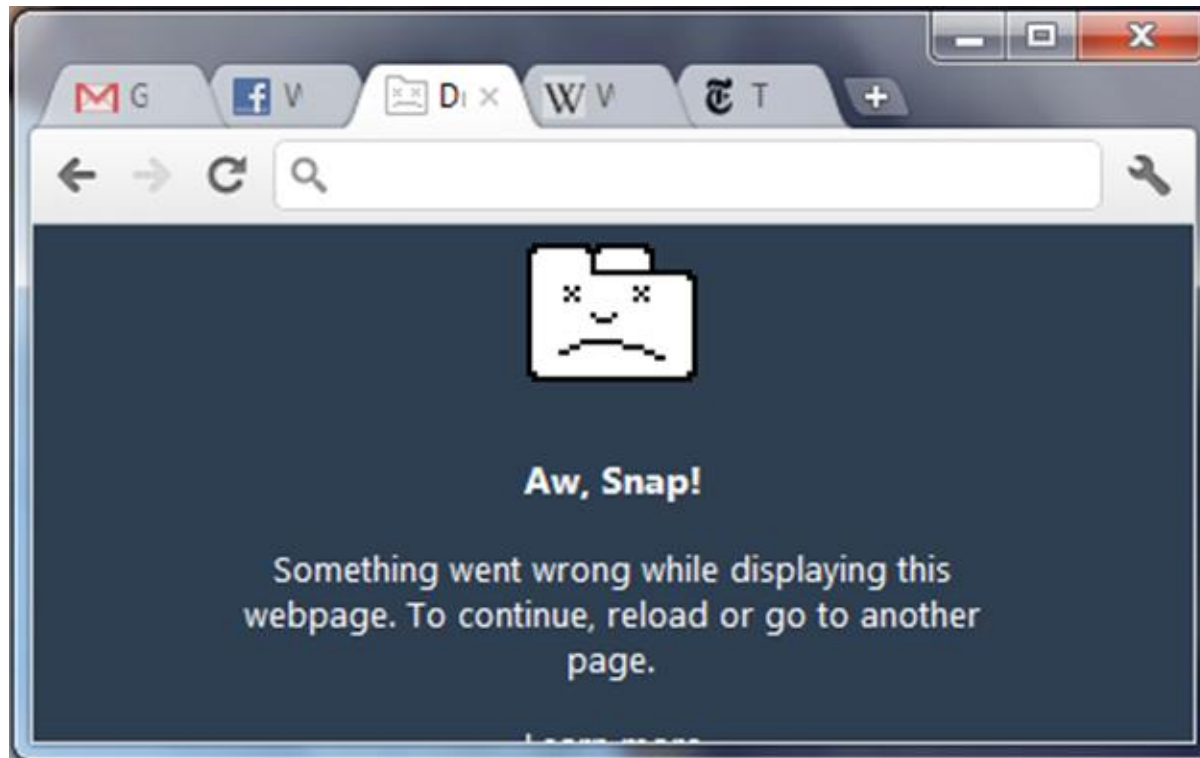


What if a webpage crashes?



Tab isolation

- ❑ Chrome brings the same isolation to webpages
- ❑ One crashed tab doesn't kill the browser



Why bother?

- ❑ Crashes mean browser bugs
- ❑ Why not just write correct code?

5,000,000

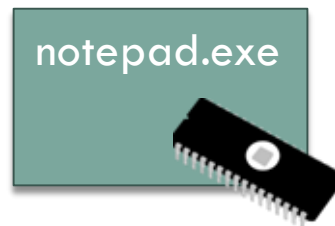
Playing in the sandbox

- How tab isolation works
- Sandboxing
- Principle of least privilege



Processes

- ❑ Tasks organized into processes
- ❑ Typically one process per application
- ❑ Each process has private memory, state, etc.
- ❑ Independently scheduled and killed



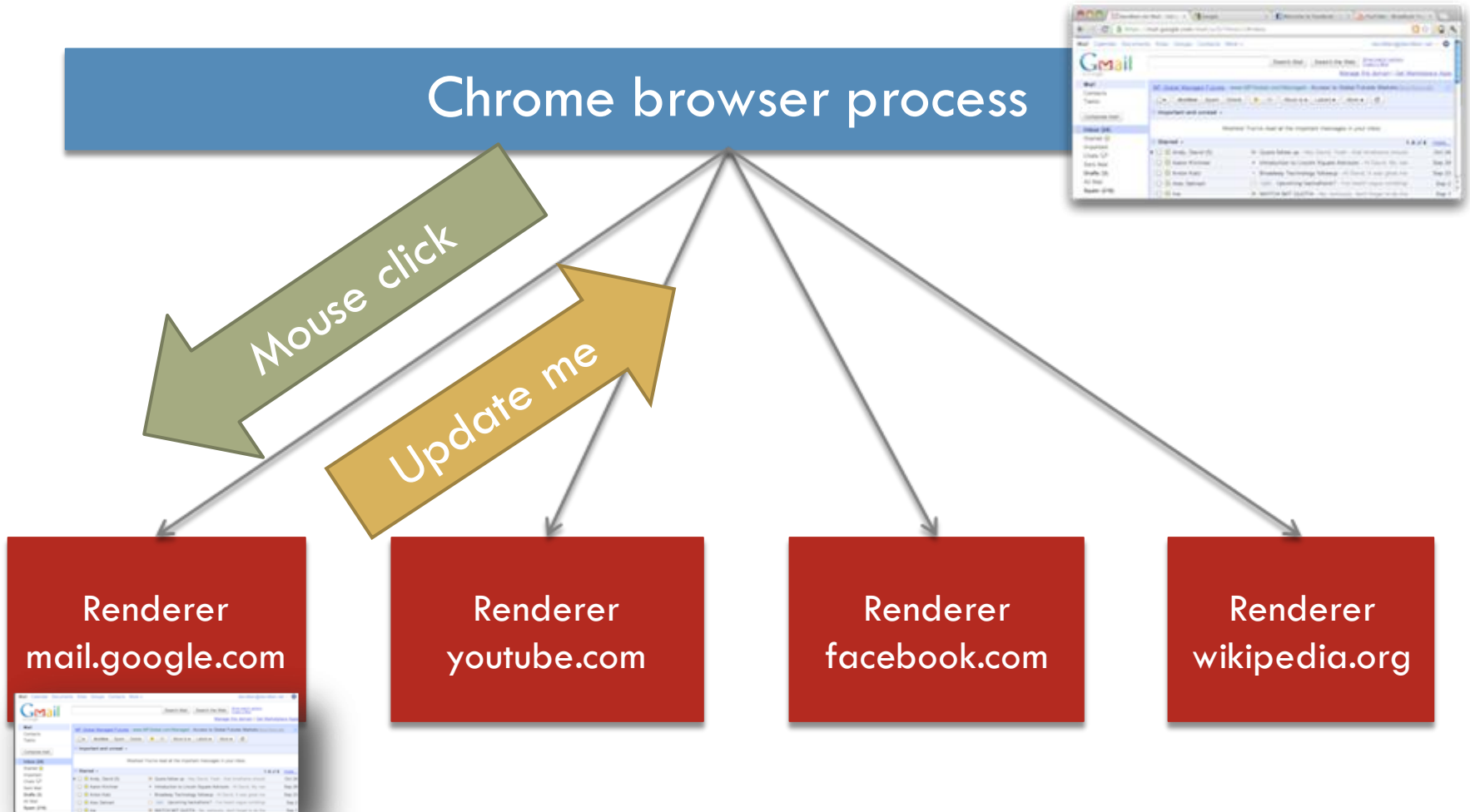
Operating System

Single-process browsing

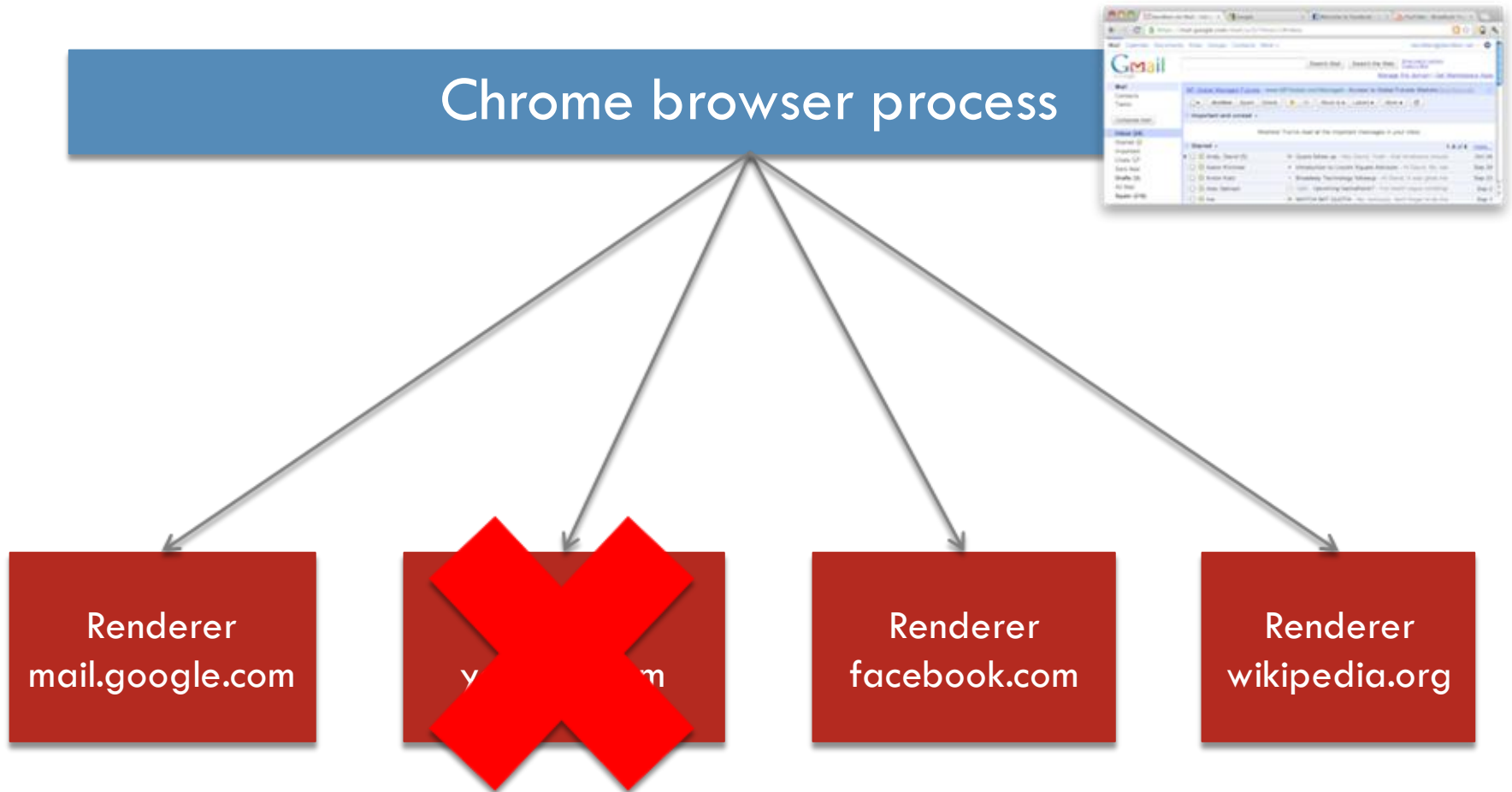
Chrome browser process



Multi-process browsing

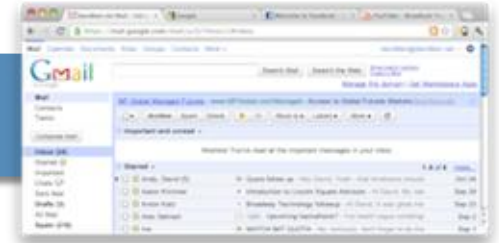


Multi-process browsing



Multi-process browsing

Chrome process



Renderer
mail.google.com

Renderer
facebook.com

Renderer
wikipedia.org

Multi-process browsing

- ❑ Each tab in a separate renderer process
- ❑ Renderers coordinated by browser process
- ❑ Communicate by sending messages
- ❑ Renderer bugs are recoverable
 - ▣ Browser process crashes are still fatal

Playing in the sandbox

- How tab isolation works
- **Sandboxing**
- Principle of least privilege



Browser security

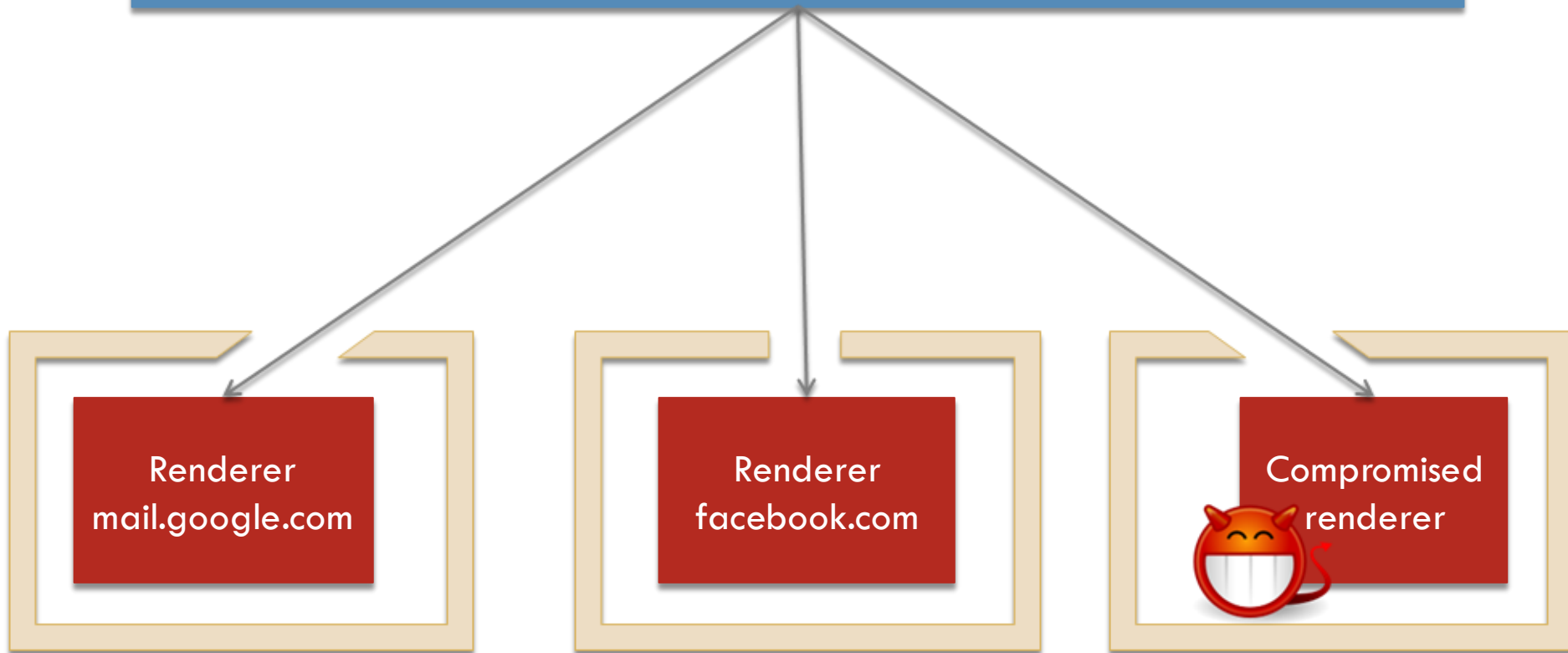
- ❑ Webpages are very restricted
 - ❑ Cannot read your English paper
 - ❑ Cannot write a virus
 - ❑ Cannot delete your files
- ❑ Visiting evil.example.com should be safe
- ❑ Browser enforces these restrictions
- ❑ What if there is a bug?

Enforcing security

- ❑ Sandbox each renderer
 - ❑ Can't access files
 - ❑ Internet
 - ❑ Other processes
- ❑ Only communicate with browser
 - ❑ Performs privileged actions on behalf of renderer
 - ❑ Including network access

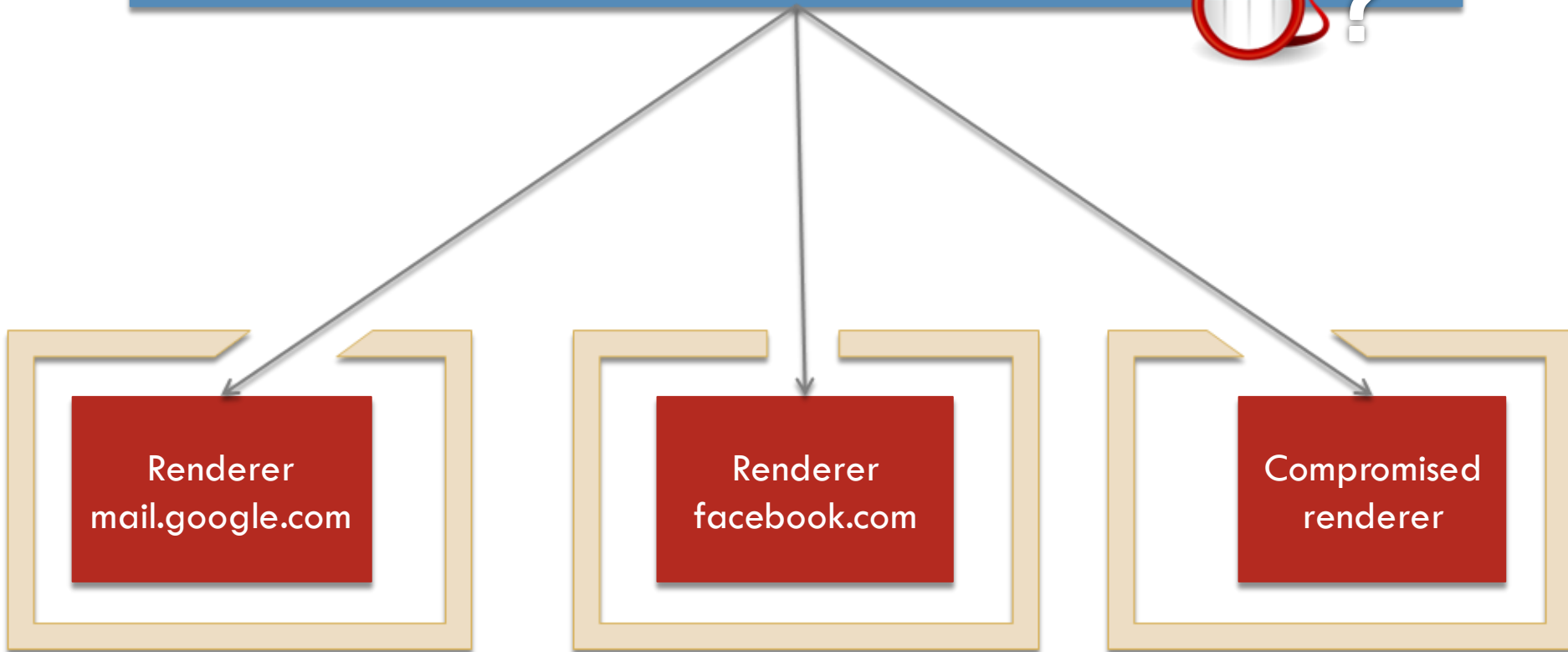
Enforcing security

Chrome browser process



Enforcing security

Chrome browser process



Playing in the sandbox

- How tab isolation works
- Sandboxing
- Principle of least privilege



Principle of least privilege



Each component of your system should have only the rights it needs and no more

- Limit damage when things go wrong
- Fewest privileges to parts most likely to fail

Playing in the sandbox

- ❑ All complex software is buggy, so design for bugs
- ❑ Separate renderer process per tab
 - ▣ Improved stability
 - ▣ Security
- ❑ Restrict renderer rights to bare minimum
- ❑ Principle of least privilege
- ❑ Questions?