

BITSQUATTING

DNS HIJACKING WITHOUT EXPLOITATION

ARTEM DINABURG

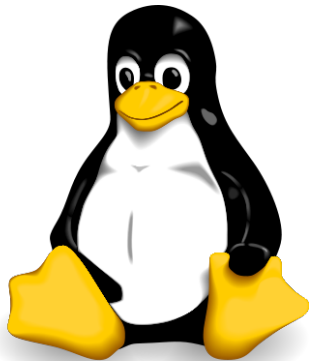
artem@dinaburg.org

artem.dinaburg@raytheon.com

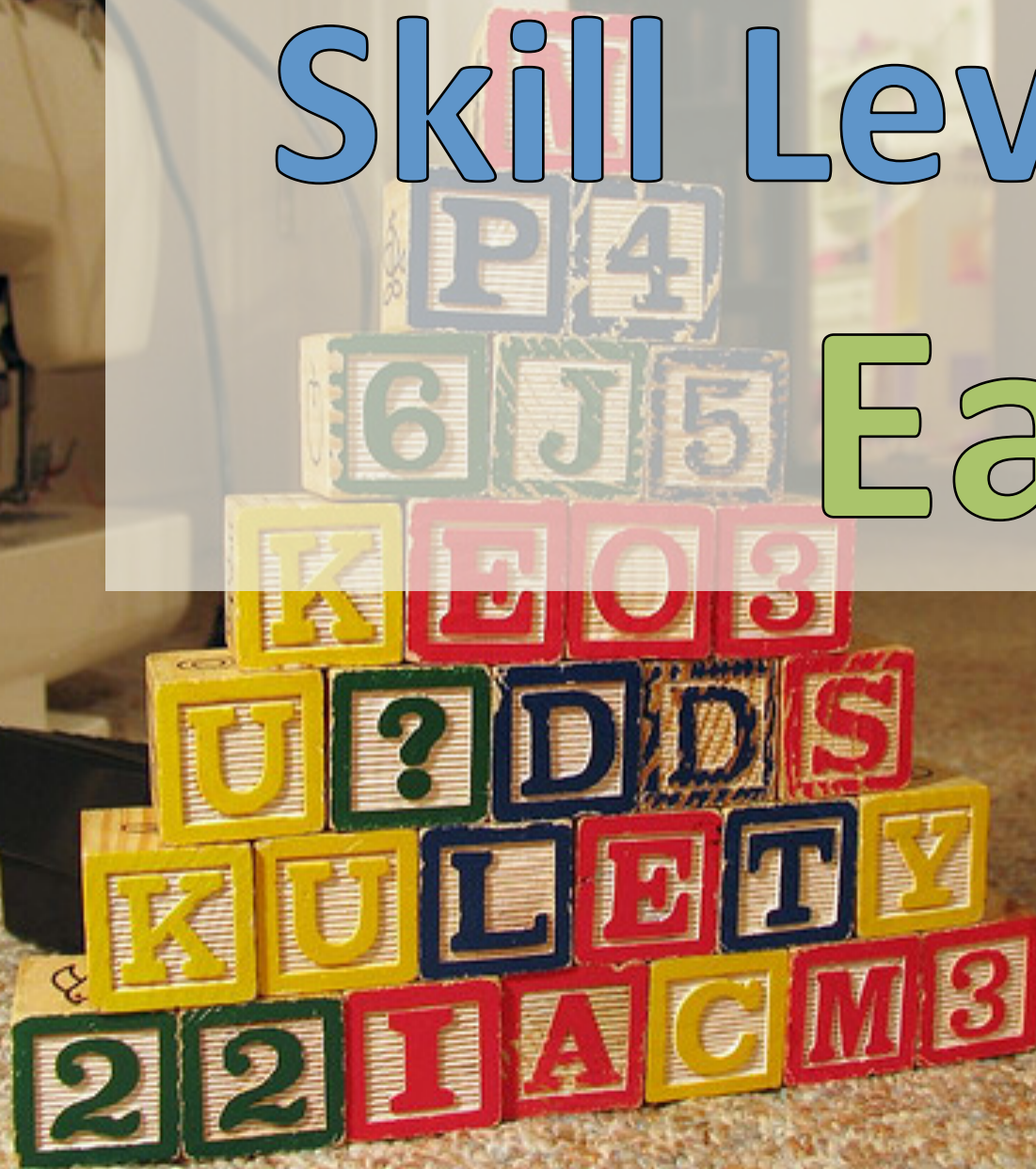
The Problem



Affected Platforms



Skill Level: Easy



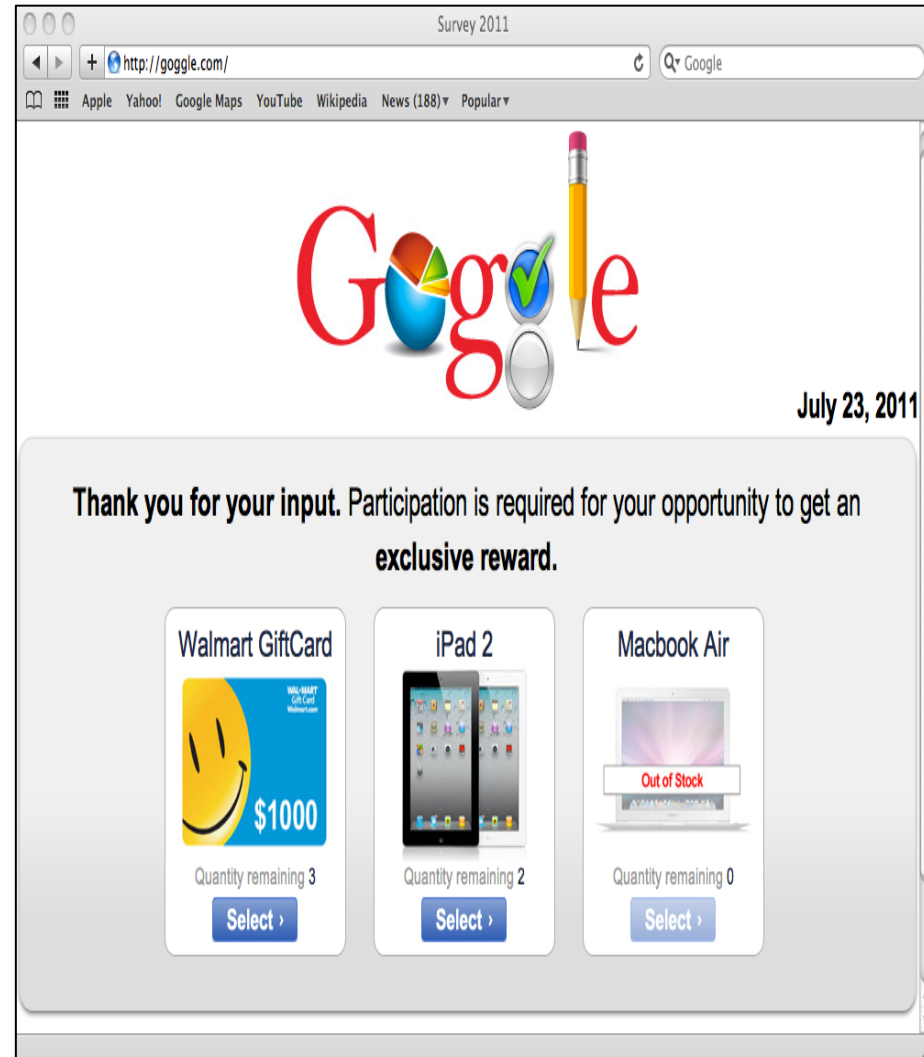
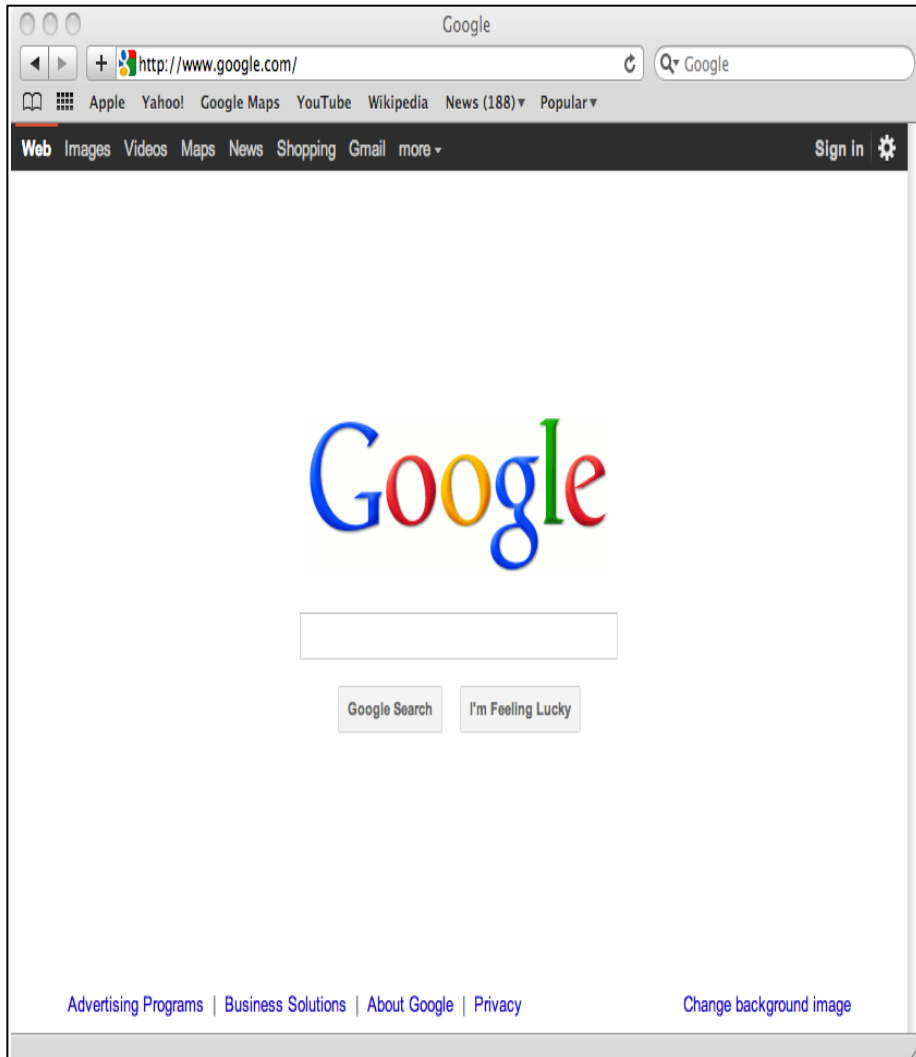


Price:
Cheap

Bitsquatting

Like typosquatting, but for bits

Typosquatting





There are

1500 daily DNS

requests per person.

Humans type

3 of them.

Computer Hardware Errors



1



0

0



1

01100011011011001101110



011000110110111101101110

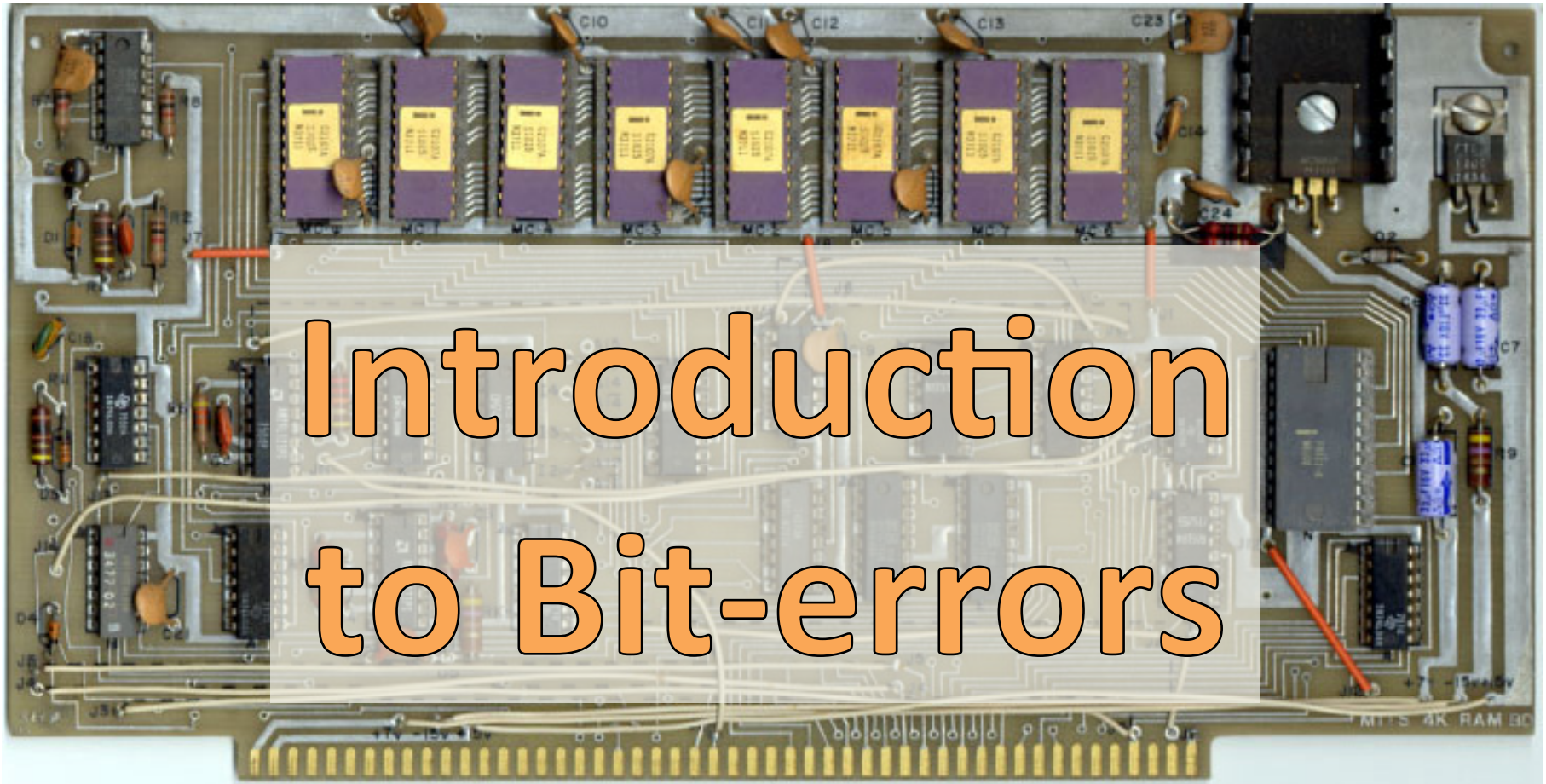
C N N . C O M

01100011011011100110111000101110011000110110111101101101



01100011011011110110111000101110011000110110111101101101

C O N . C O M



Introduction to Bit-errors

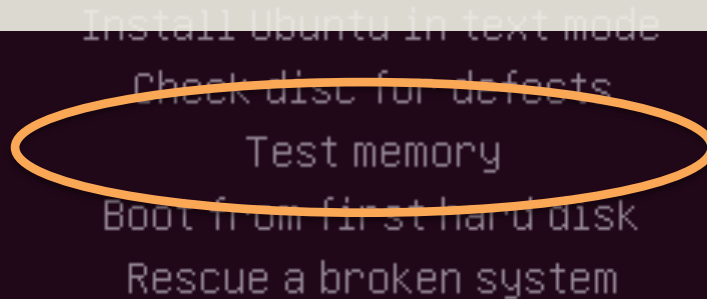
MITS Altair 8800 4K Ram Board, Rev 0 with 8 Intel C2107A DRAMs

MITS Altair RAM board image © 2005 George M. Phillips Jr.



Cache
Contamination

Ubuntu install CDs come with Memtest86



```

Memtest86 v1.70 | Pass 43% #####
Athlon XP (0.13) 2092 MHz | Test 13% #####
L1 Cache: 128K 12832MB/s | Test #6 [Moving inversions, 32 bit pattern]
L2 Cache: 512K 4085MB/s | Testing: 120K - 1024M 1024M
Memory : 1024M 1009MB/s | Pattern: 00000010
Chipset : nVidia nForce2 SPP / FSB : 199 MHz
Settings: RAM : 199 MHz (DDR398) / CAS : 3-3-3-8 / Single Channel (64 bits)

WallTime  Cached  RsvdMem  MemMap  Cache  ECC  Test  Pass  Errs  ECC  Errs
-----
0:46:22  1024M      84K      82M      148      0

Tst  Pass  Failing Address  Good  Bad  Err-Bits  Count Chan
---
6    1    00036bb802 - 875.5MB 00020000 00020200 00000200 1
6    1    00036bb802 - 875.5MB 00080000 00080800 00000800 1
6    1    00036bb803c - 875.5MB 00080000 00080800 00000800 1
6    1    00037eb8024 - 894.5MB 00002000 00002020 00000020 1
6    1    00037eb802c - 894.5MB 00008000 00008080 00000080 1
6    1    0003b7b8024 - 951.5MB 00002000 00000000 00002000 1
6    1    0003b7b802c - 951.5MB 00008000 00000000 00008000 1
6    1    0003b7b8034 - 951.5MB 00020000 00020200 00000200 1
6    1    0003b7b803c - 951.5MB 00080000 00080800 00000800 1

(ESC)Reboot (c)configuration (SP)scroll_lock (CR)scroll_unlock

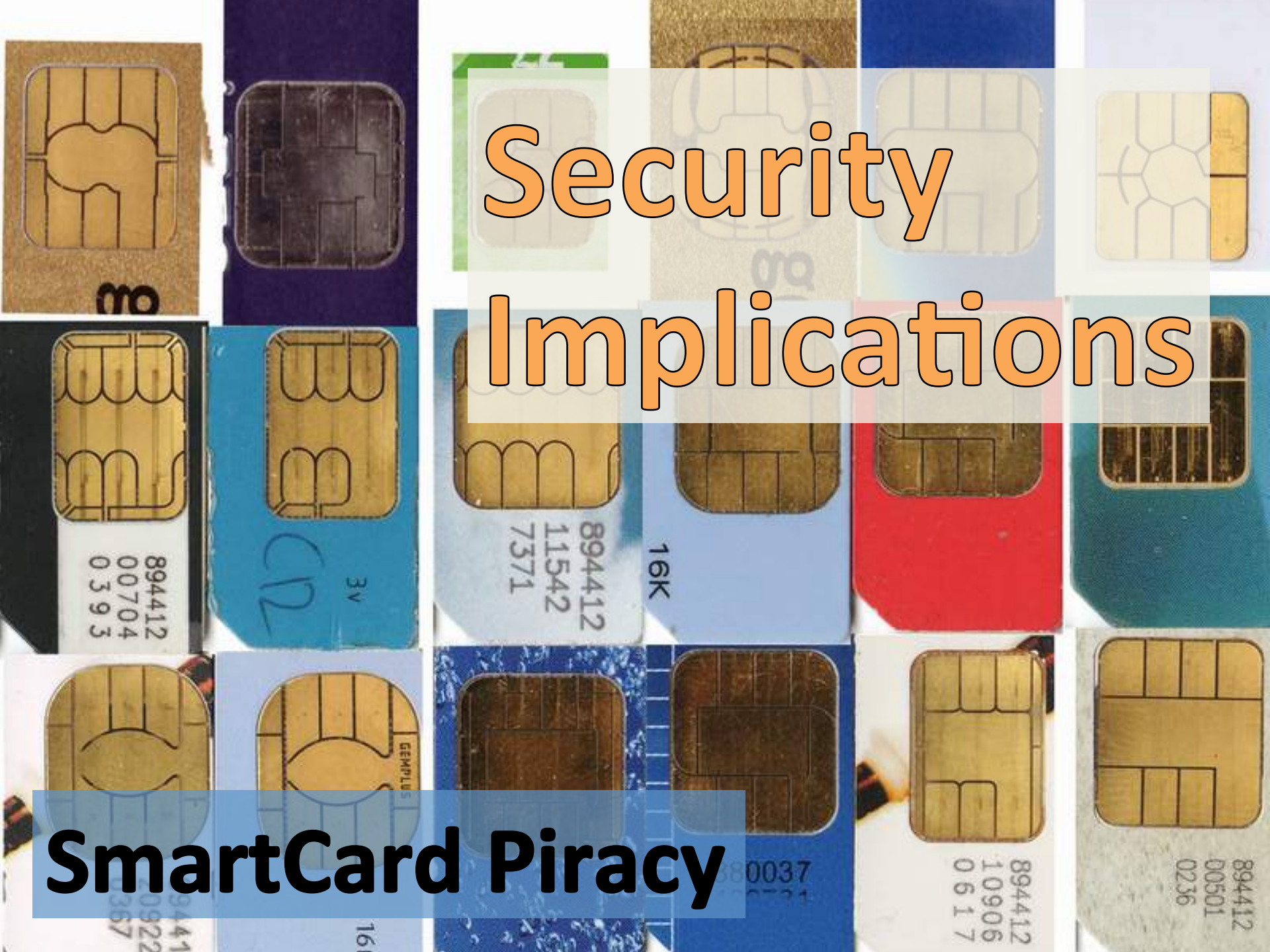
```

...because of
hardware errors

A grayscale photograph of an open server rack. In the foreground, a digital multimeter is visible, displaying '54C' on its screen. The server rack is open, revealing internal components like circuit boards and cables. A large, semi-transparent white box with orange text is overlaid on the right side of the image.

Security Implications

JVM Sandbox Escape



Security Implications

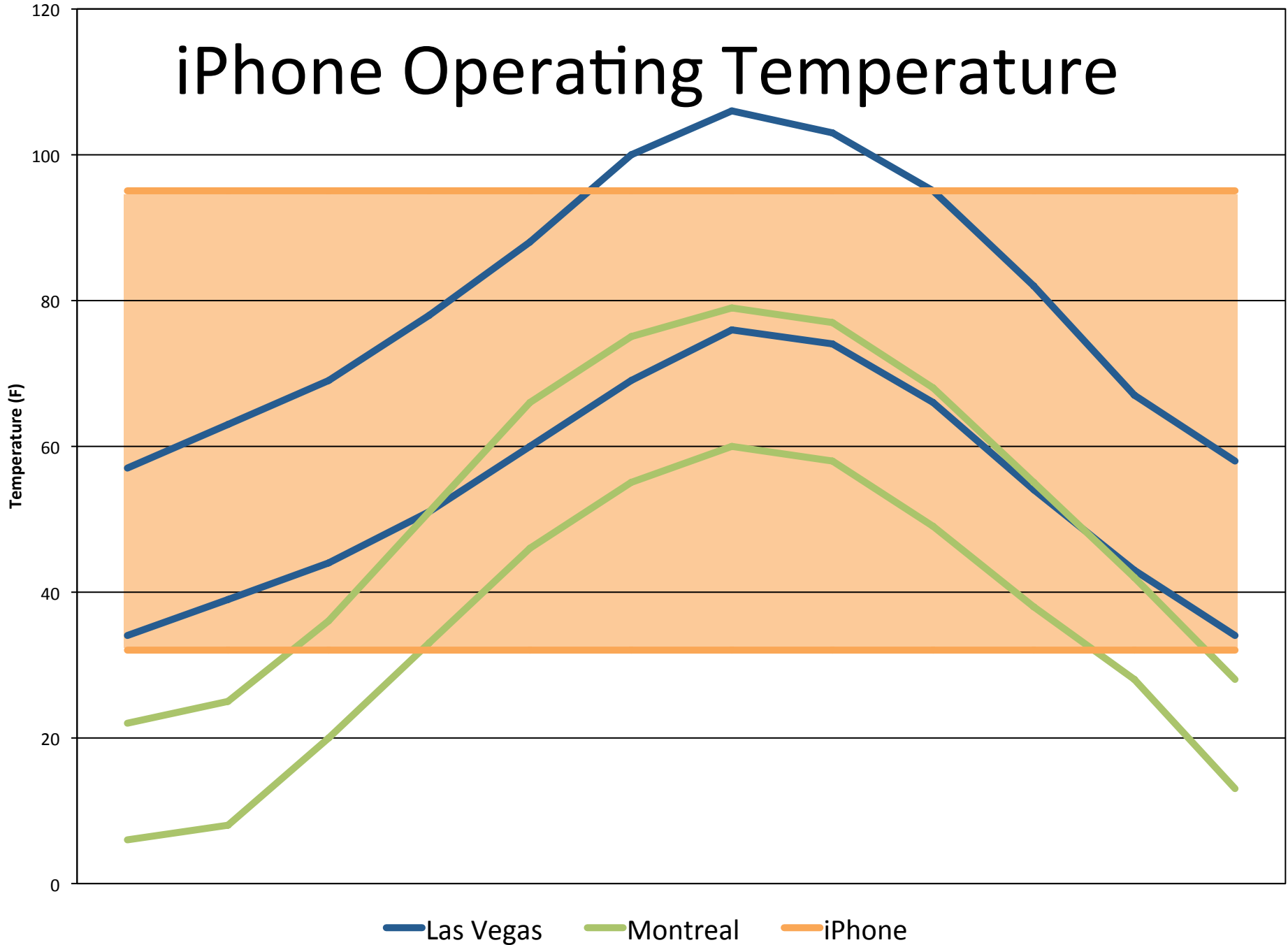
SmartCard Piracy

CAUSES OF BIT-ERRORS:

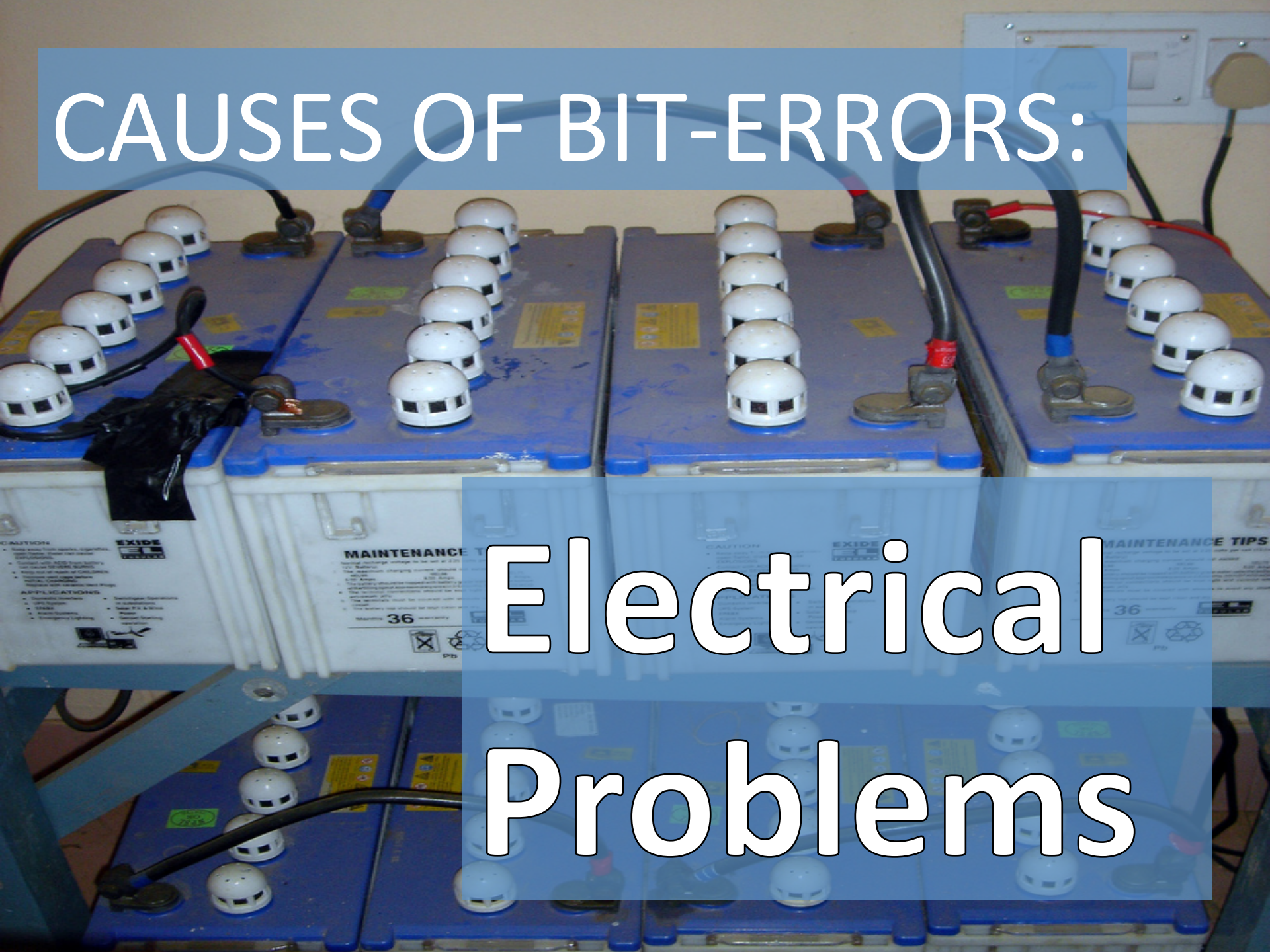


Heat

iPhone Operating Temperature



CAUSES OF BIT-ERRORS:



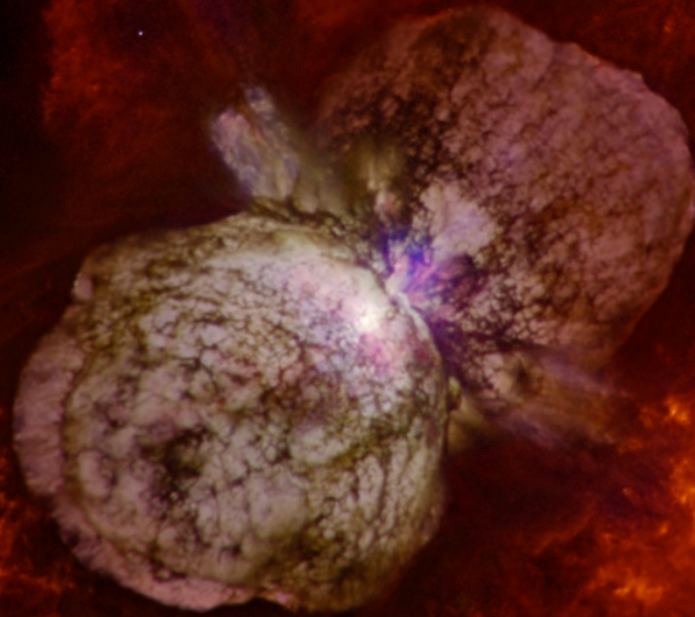
Electrical Problems

CAUSES OF BIT-ERRORS:

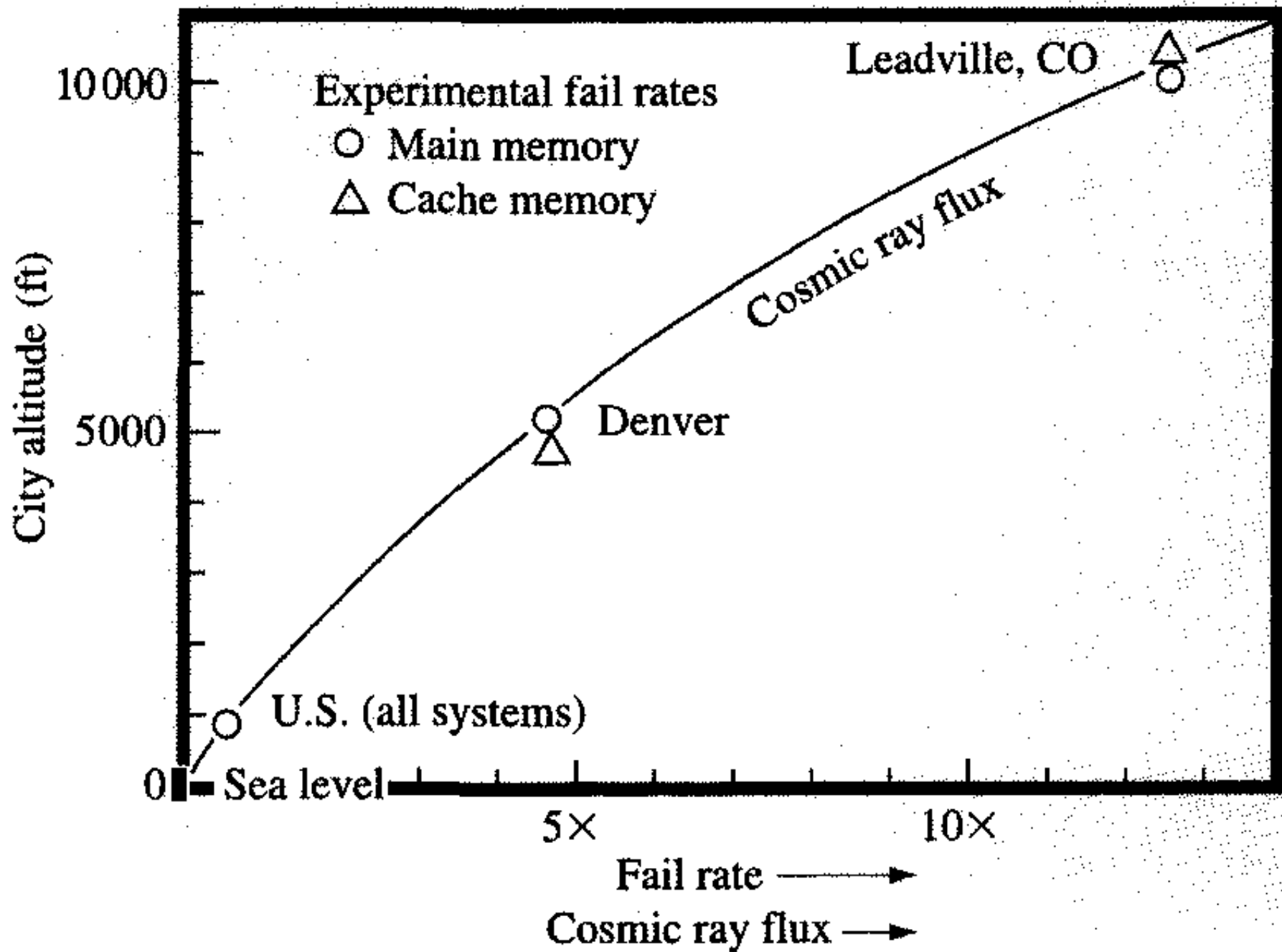
Defects



CAUSES OF BIT-ERRORS:



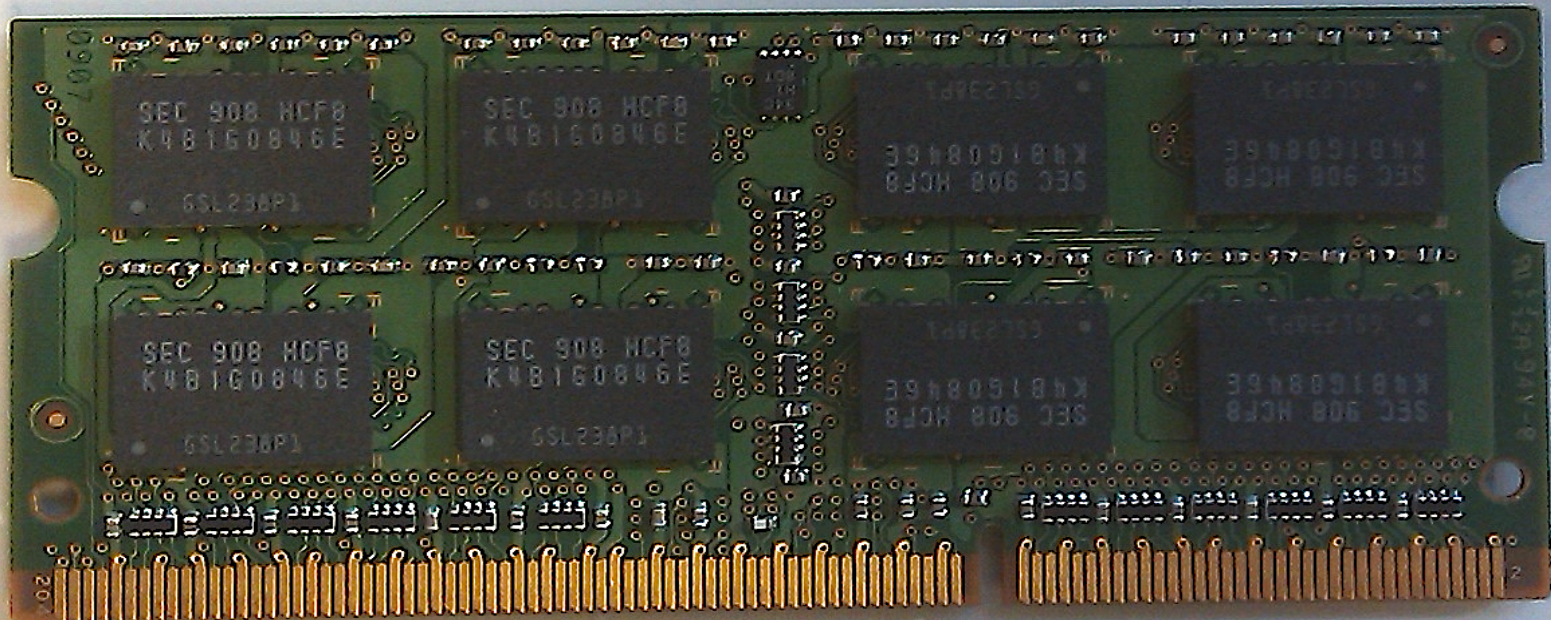
Cosmic Rays

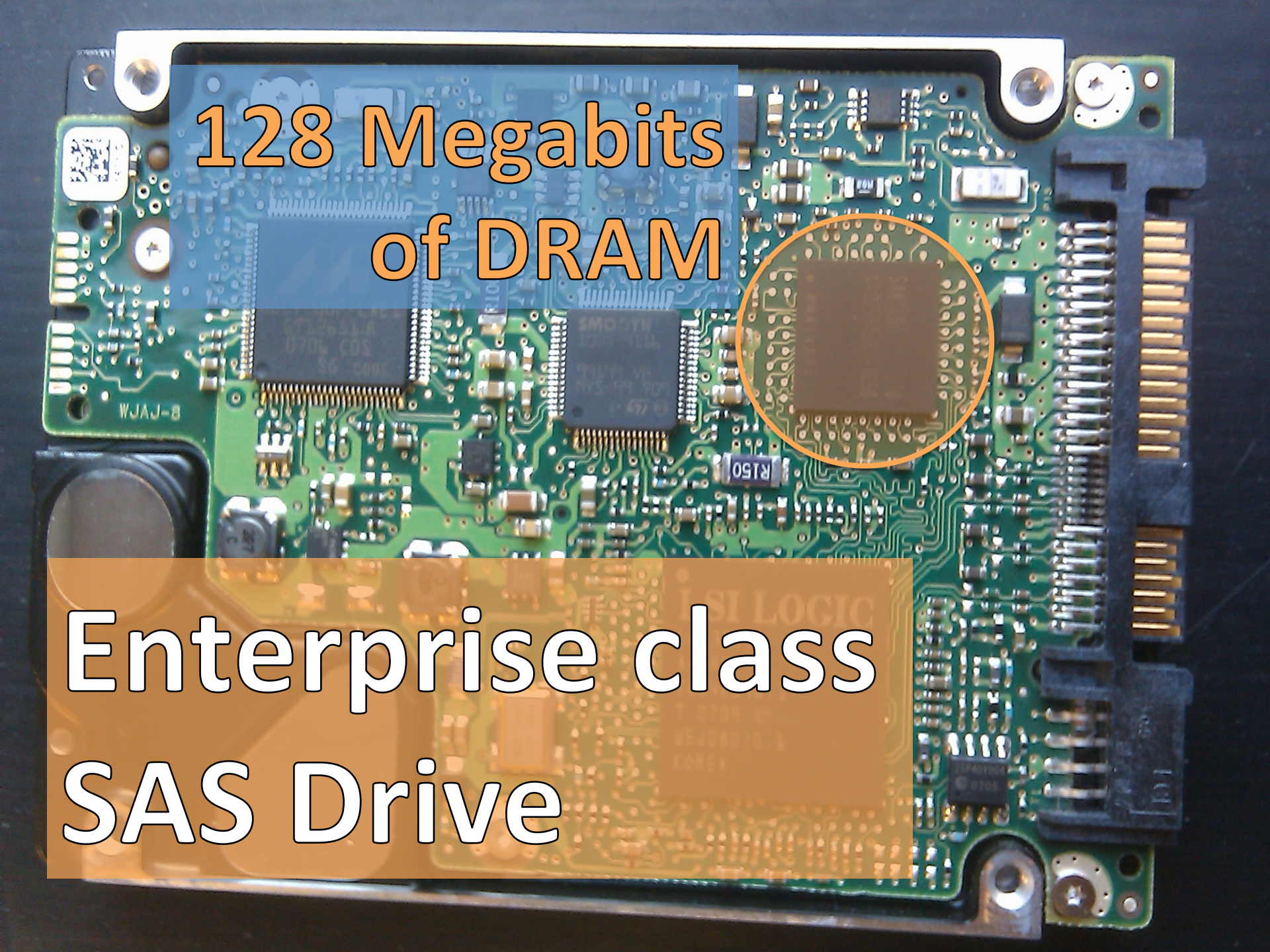




What's the
real cause?

Let's talk about DRAM



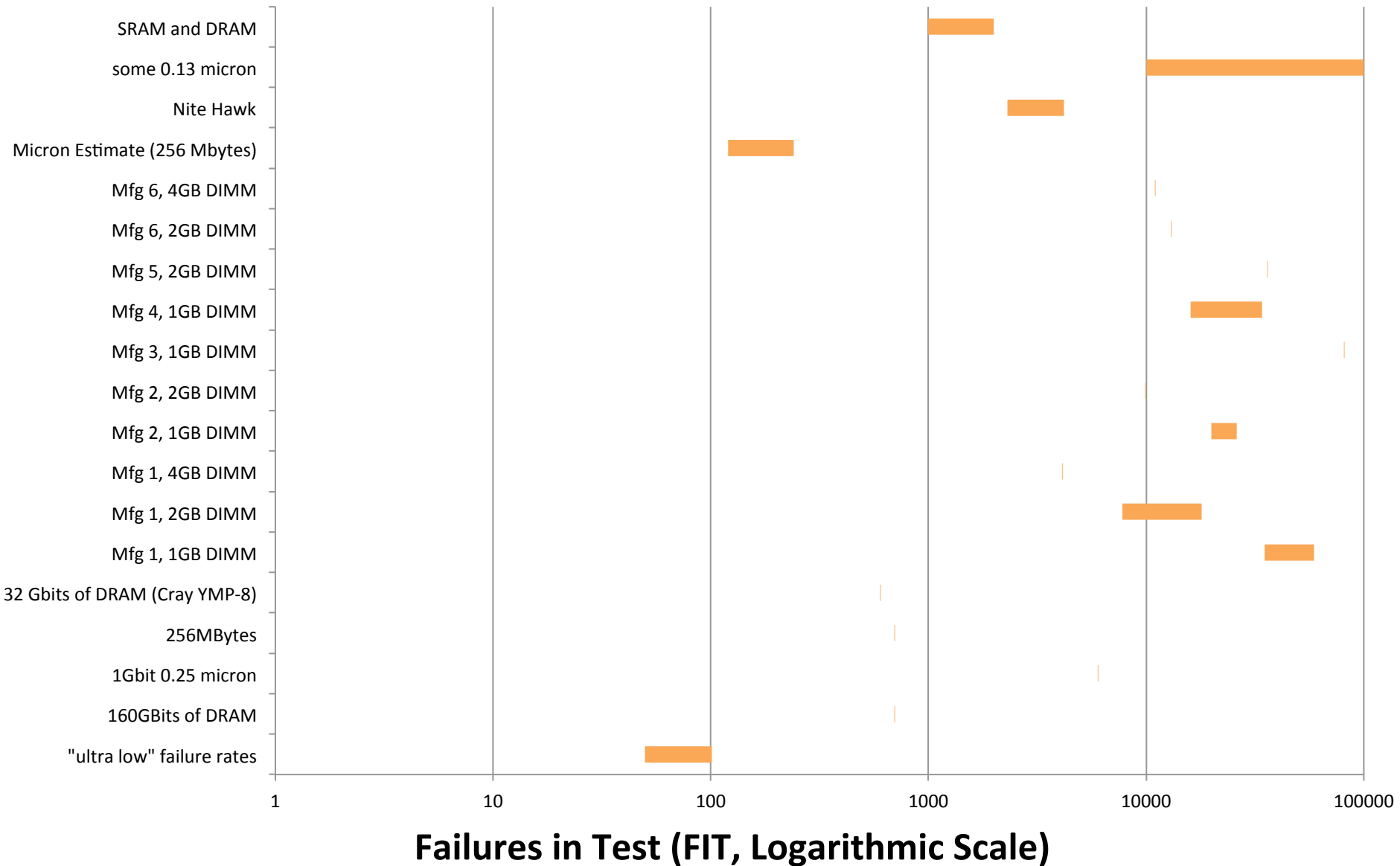


128 Megabits
of DRAM

The image shows a green printed circuit board (PCB) for an enterprise-class SAS drive. It features a large black DRAM chip in the center, a smaller black chip to its left, and a large black chip to its right which is circled in orange. The board is populated with various electronic components, including resistors, capacitors, and integrated circuits. A multi-pin connector is visible on the right side of the board. The text '128 Megabits of DRAM' is overlaid in orange on a blue background in the upper left. The text 'Enterprise class SAS Drive' is overlaid in white on an orange background in the lower left.

Enterprise class
SAS Drive

DRAM Failure Rates



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

MACHINE_CHECK_EXCEPTION

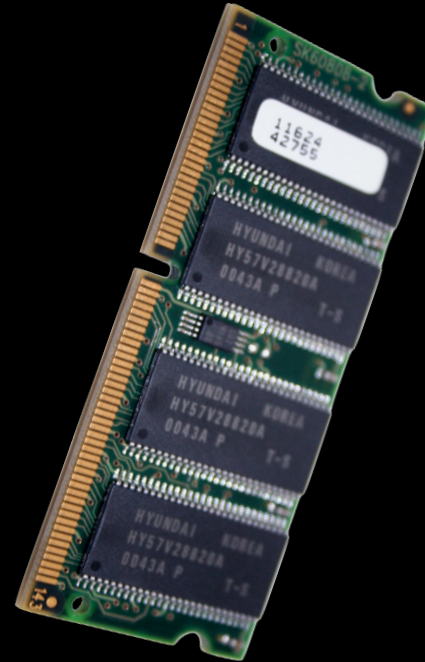
If this is the first time you've seen this stop error screen, restart your computer. If the screen appears again, follow these steps:

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.

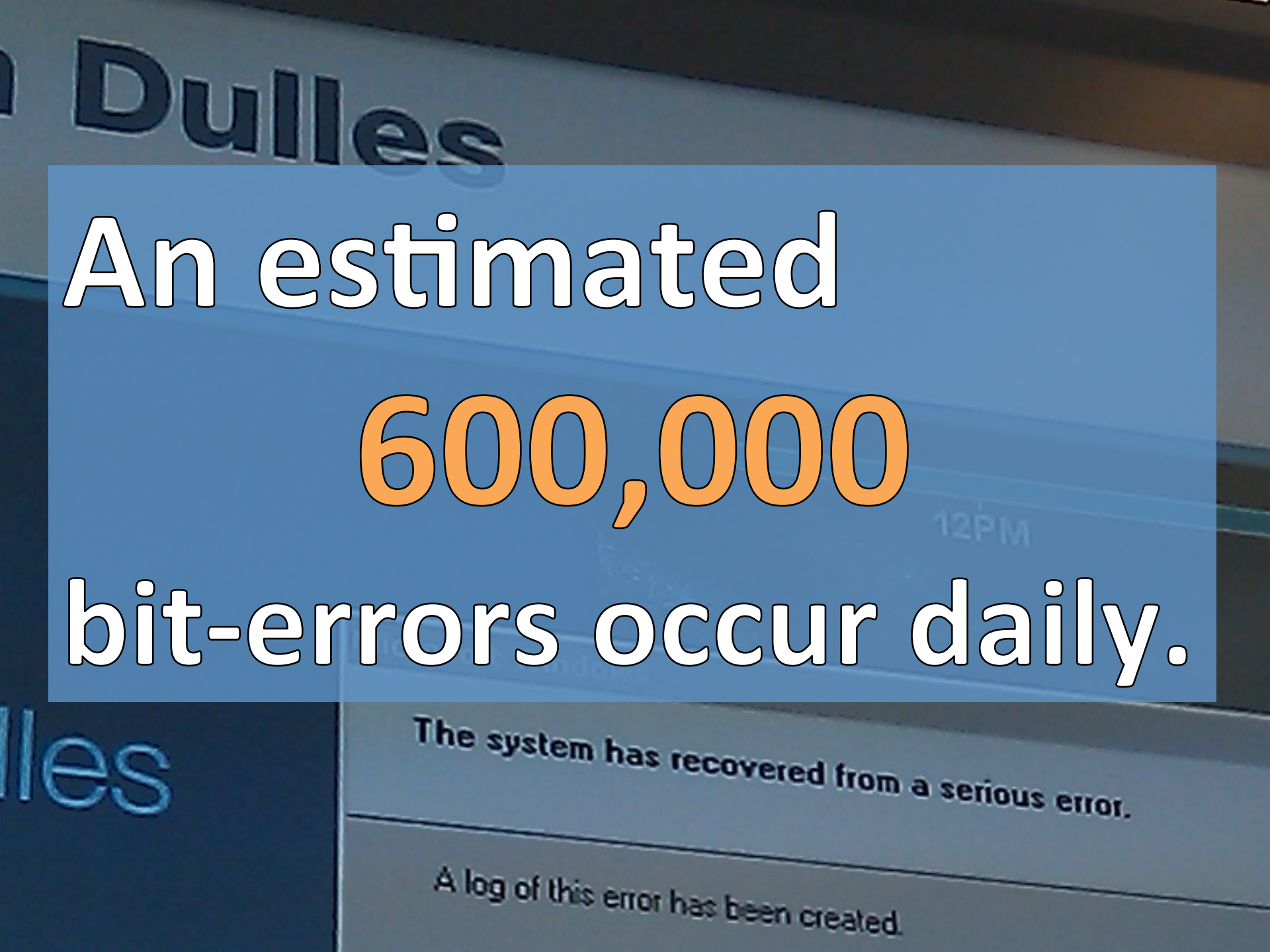
If the problem is caused by a recently installed hardware or software, disable BIOS memory options such as caching or shadowing. If you need to use safe Mode to remove or disable components, restart your computer, press F8 to select Advanced startup options, and then select safe Mode.

Technical information:

*** STOP: 0x0000009C (0x00000004, 0x8086EFF0, 0xB2000000, 0x00070F0F)



600 PiB

The background is a photograph of a computer monitor. At the top, the word 'Dulles' is visible in a large, blue, sans-serif font. Below it, a blue semi-transparent rectangular box contains the main text of the slide. At the bottom of the screen, a system error message is displayed in a smaller, black, sans-serif font.

An estimated
600,000
bit-errors occur daily.

The system has recovered from a serious error.

A log of this error has been created.

Experiment: Step 1

ikamai.net

aeazon.com

a-azon.com

amazgn.com

microsmft.com

micrgsoft.com

miarosoft.com

iicrosoft.com

microsnft.com

mhcrosoft.com

eicrosoft.com

mic2osoft.com

micro3oft.com

doublechick.net

do5bleclick.net

doubleslick.net

li6e.com

0mdn.net

2-dn.net

2edn.net

2ldn.net

2mfn.net

2mln.net

2odn.net

6mdn.net

fbbdn.net

fbgdn.net

gbcndn.net

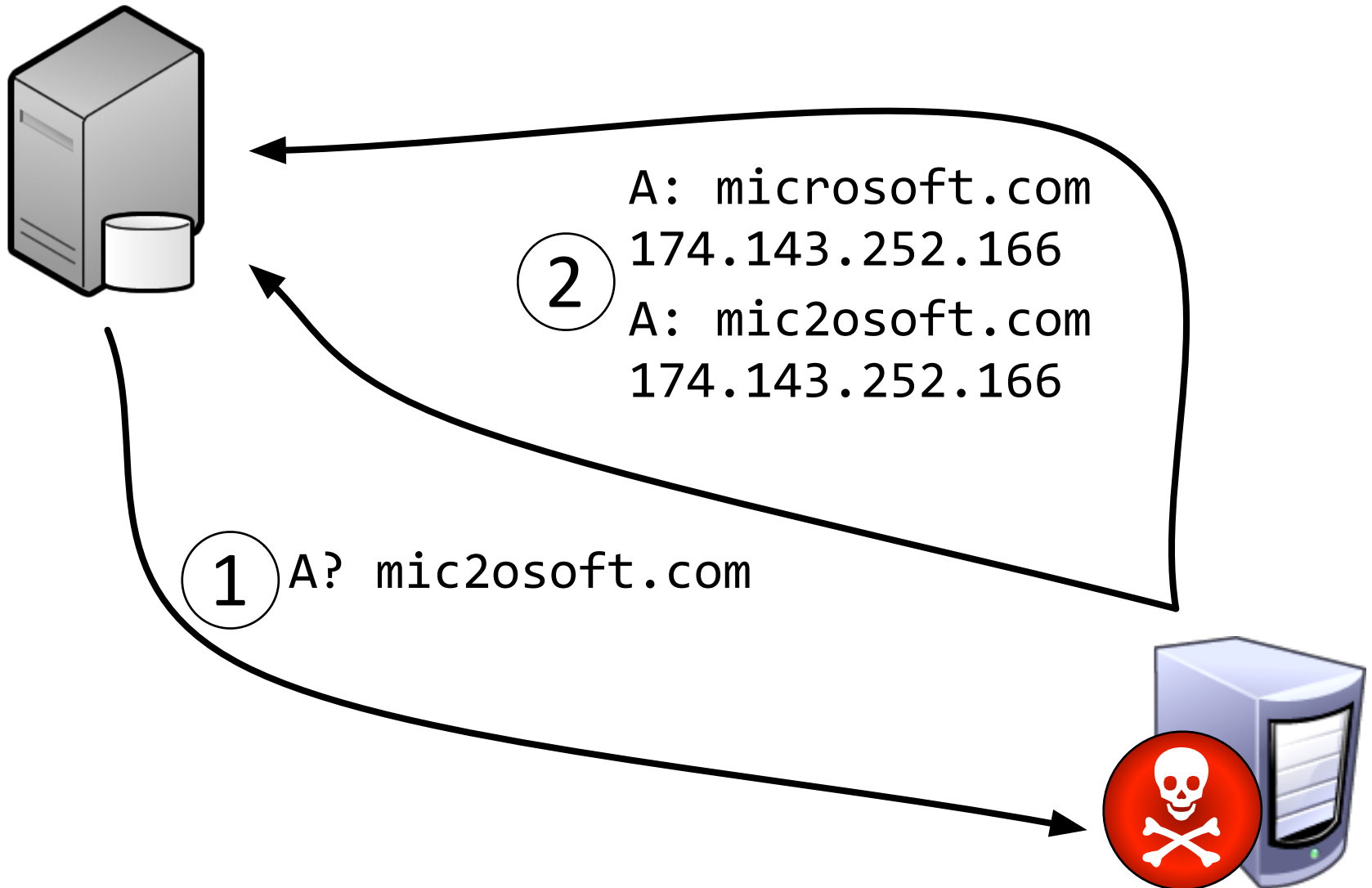
fjcdn.net

dbcdn.net

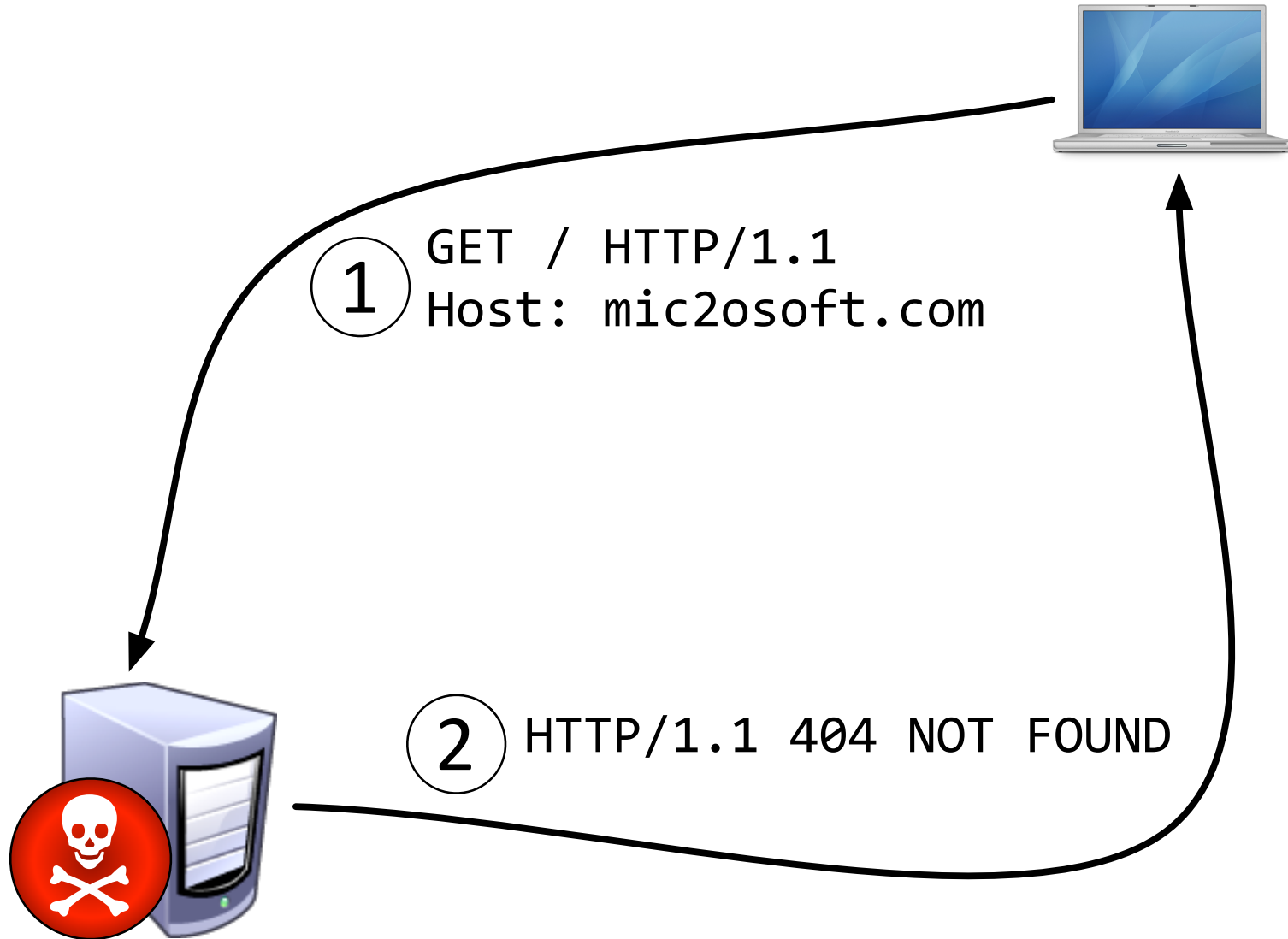
roop-servers.net

gmam1.com

Experiment, Step 2



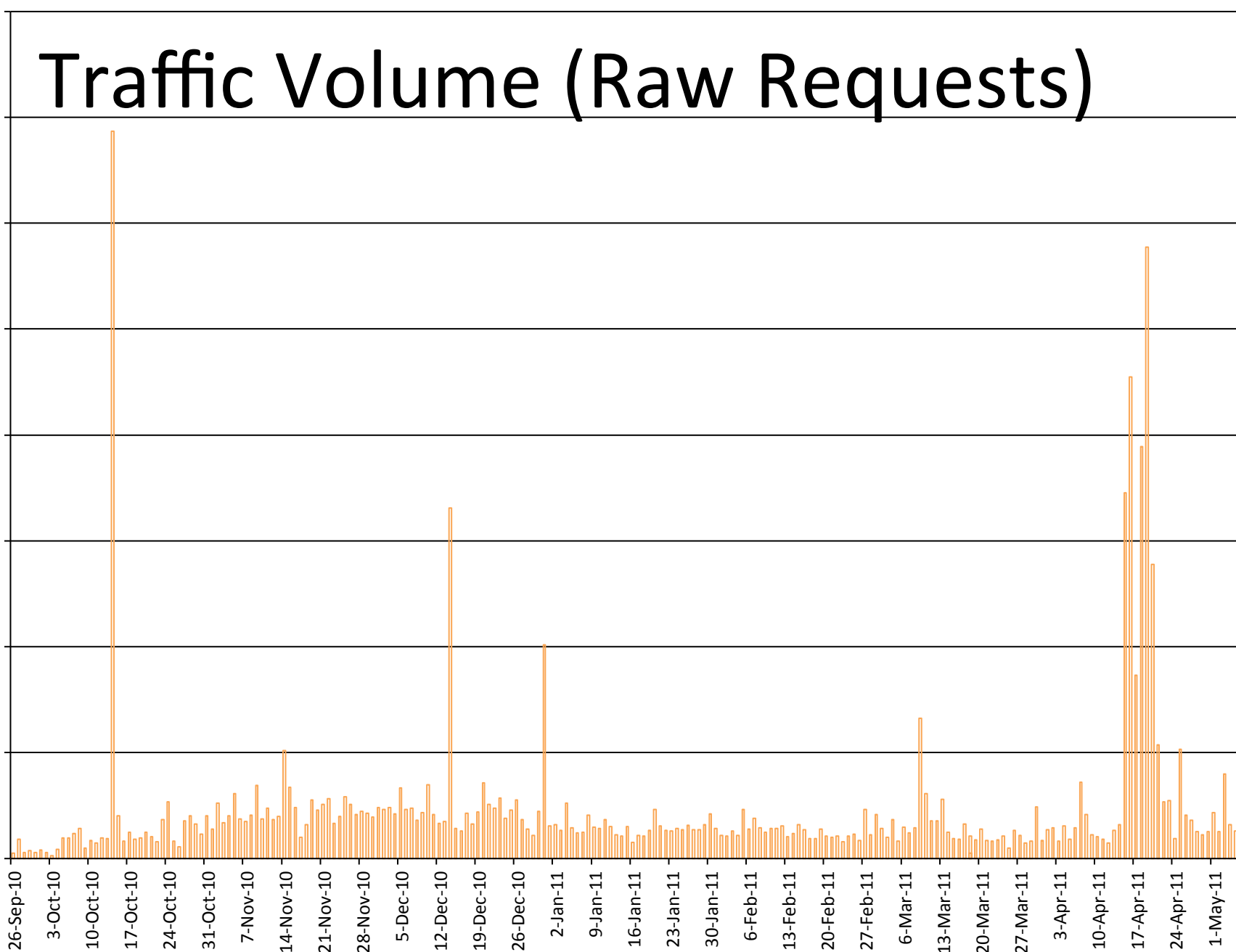
Experiment, Step 3



Traffic Volume (Raw Requests)

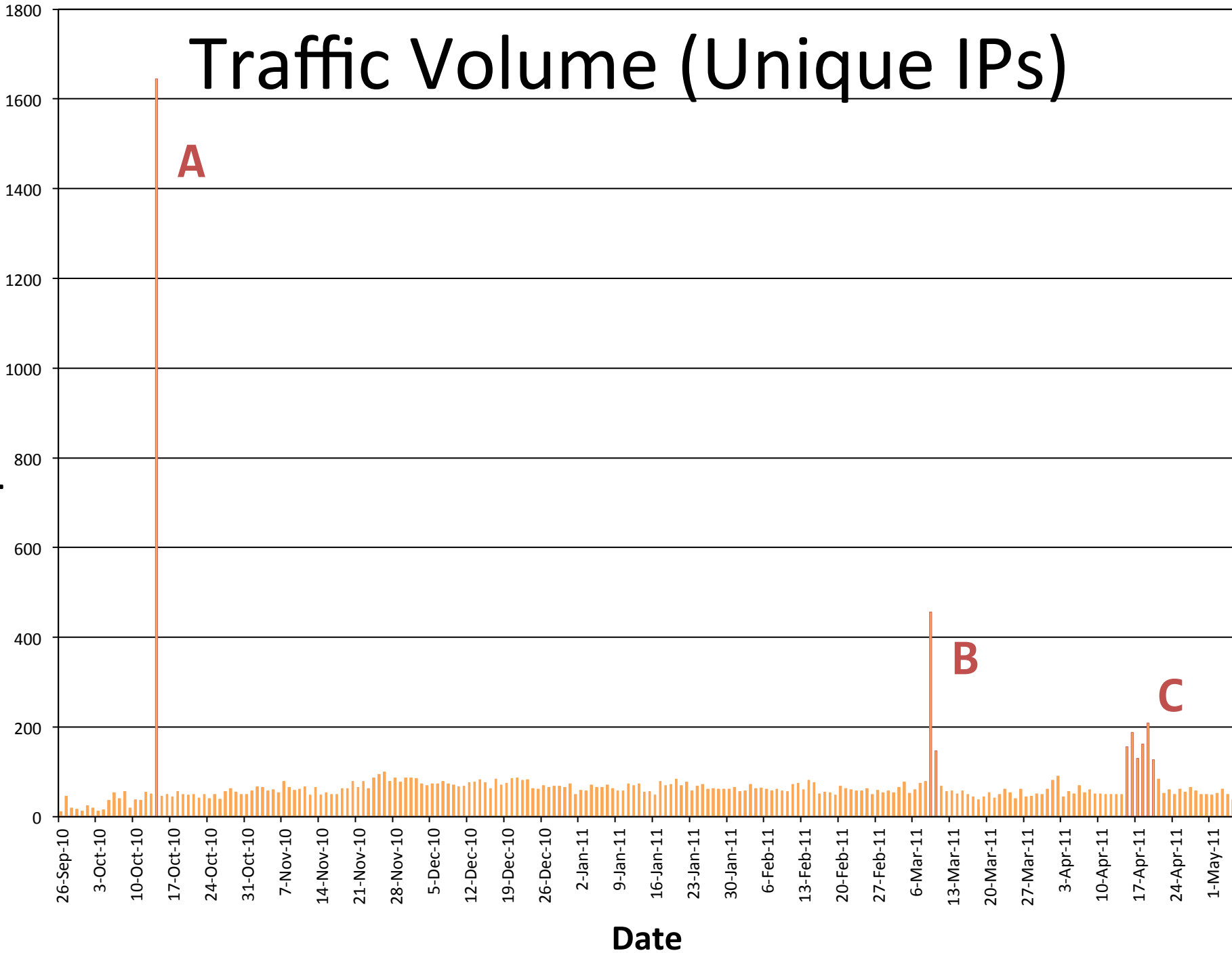
Number of Requests

Date

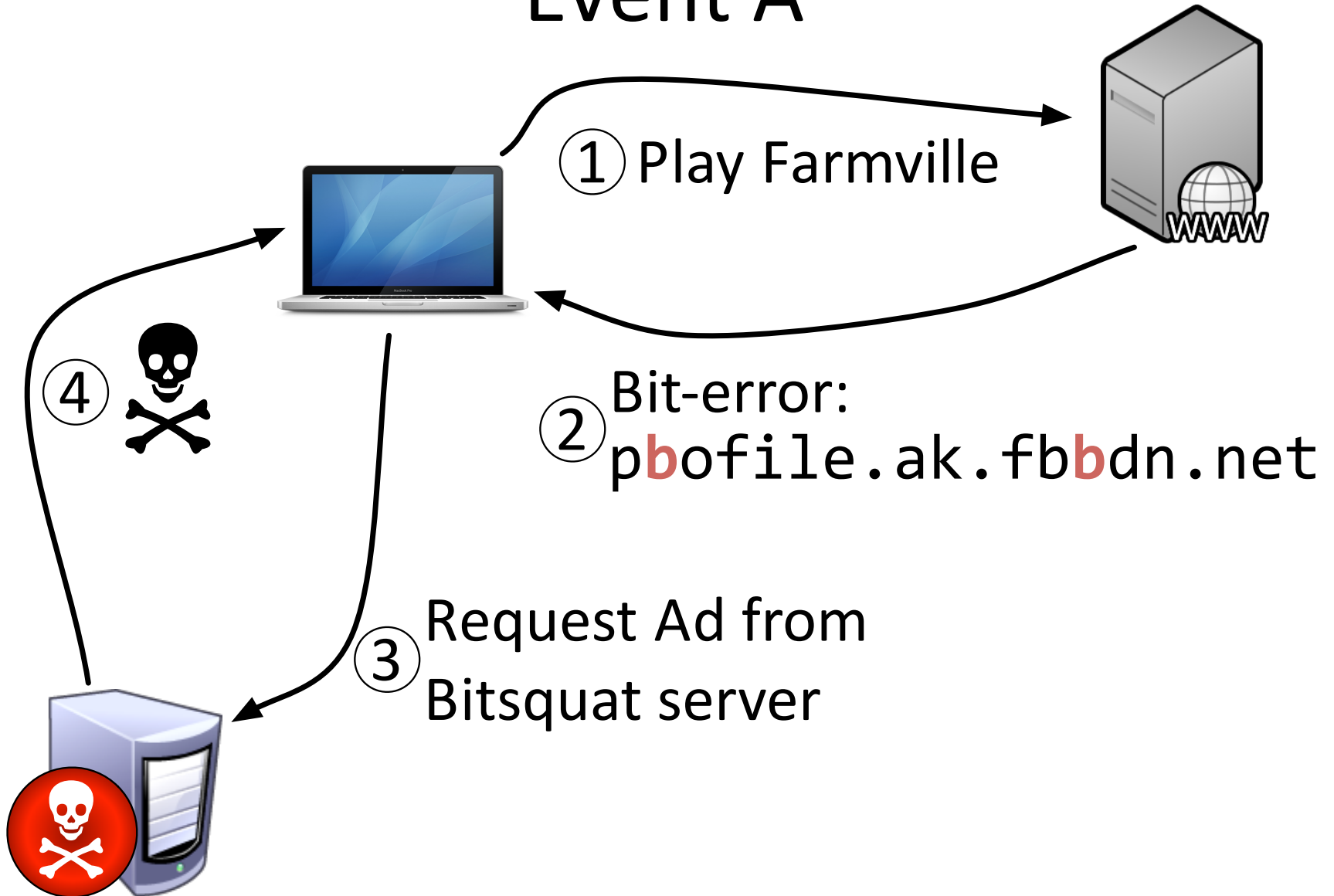


Traffic Volume (Unique IPs)

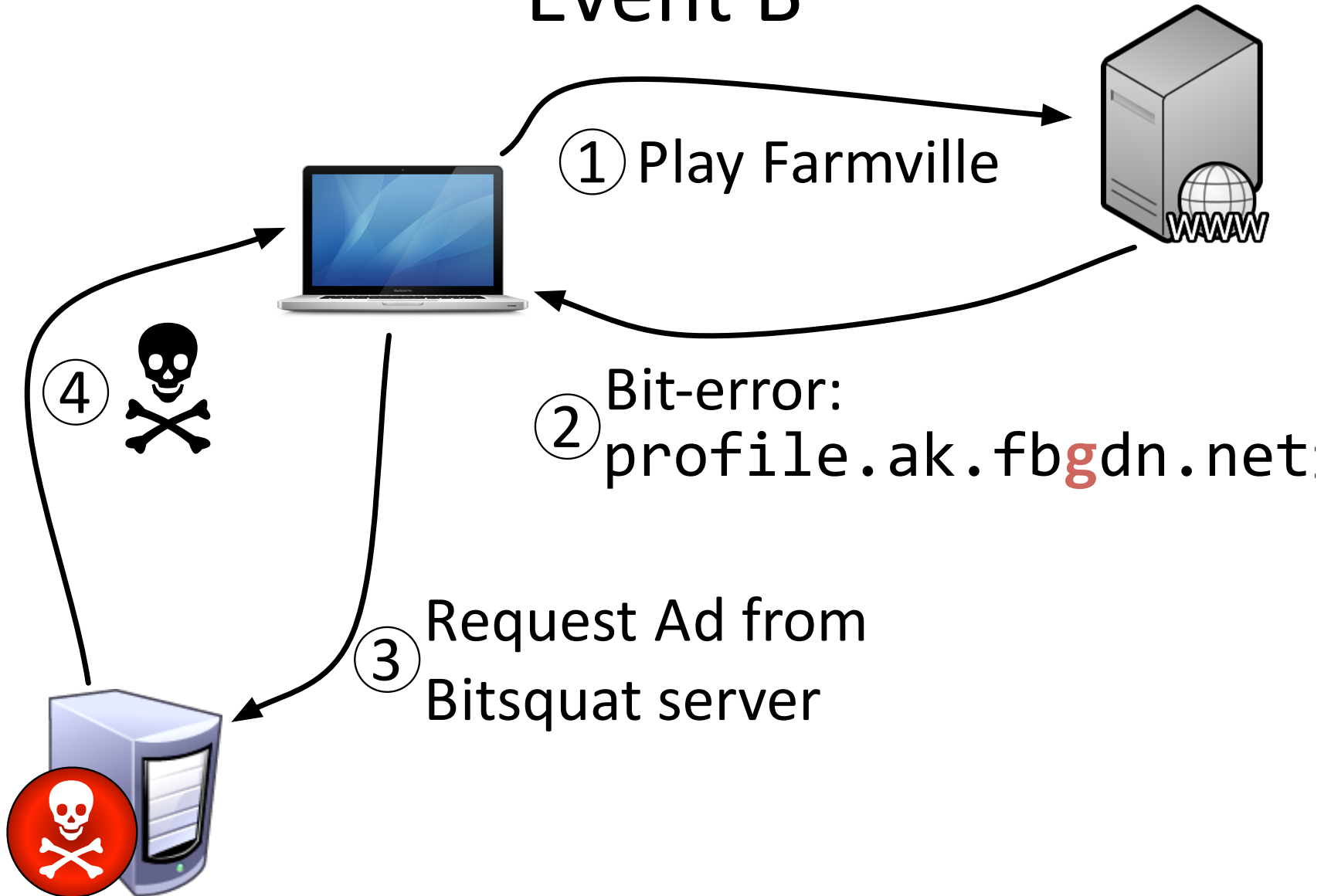
Unique IPs



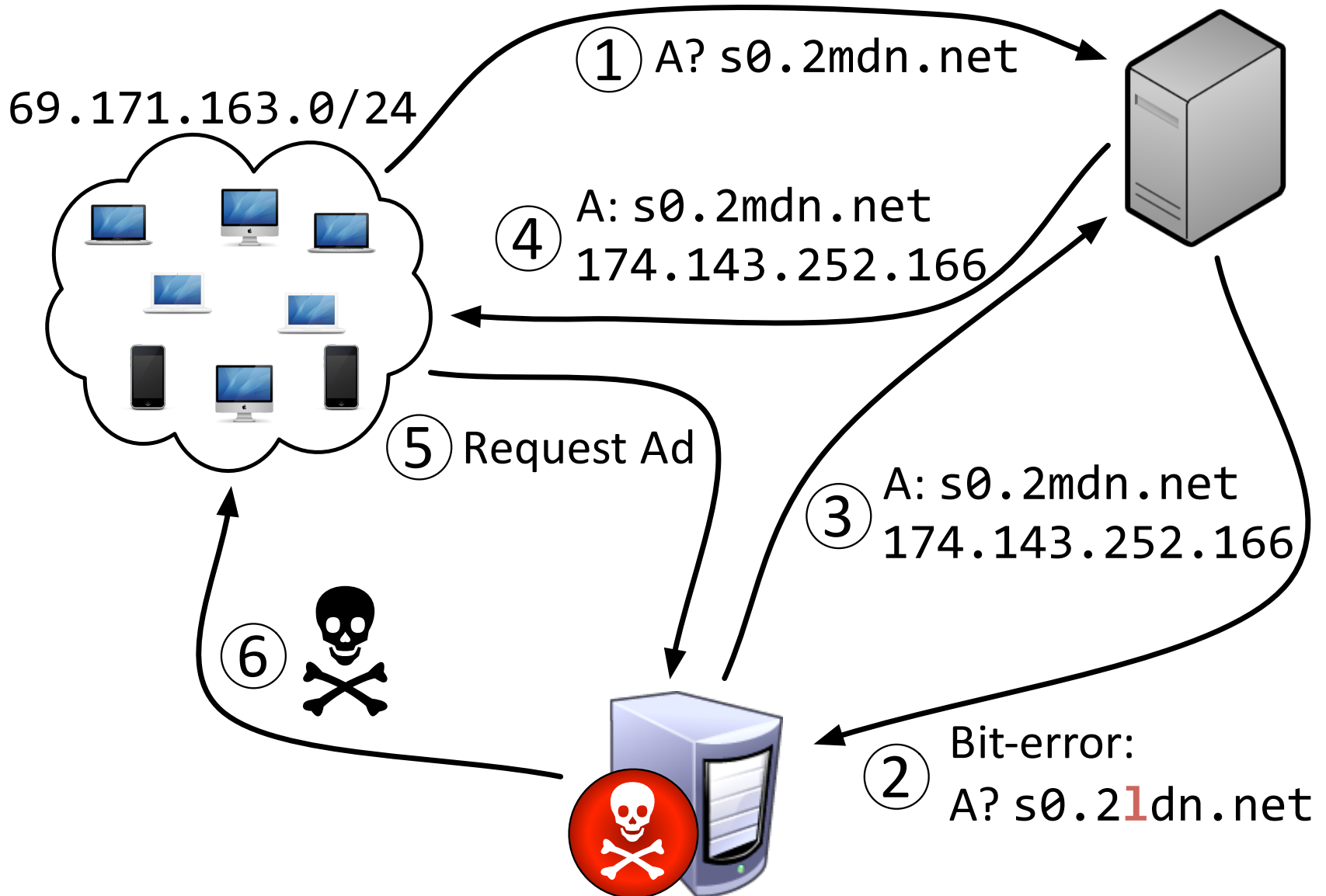
Event A



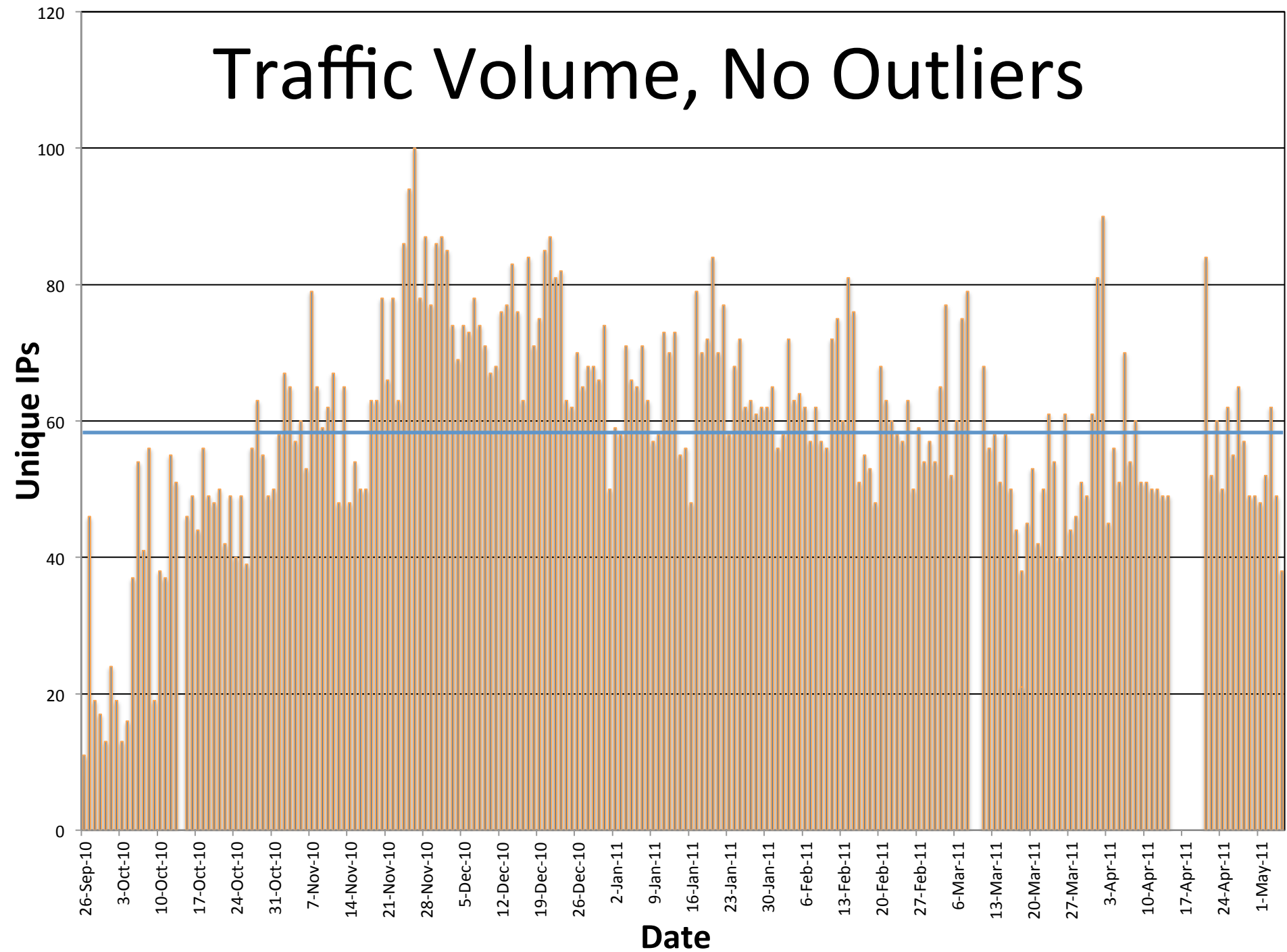
Event B



Event C

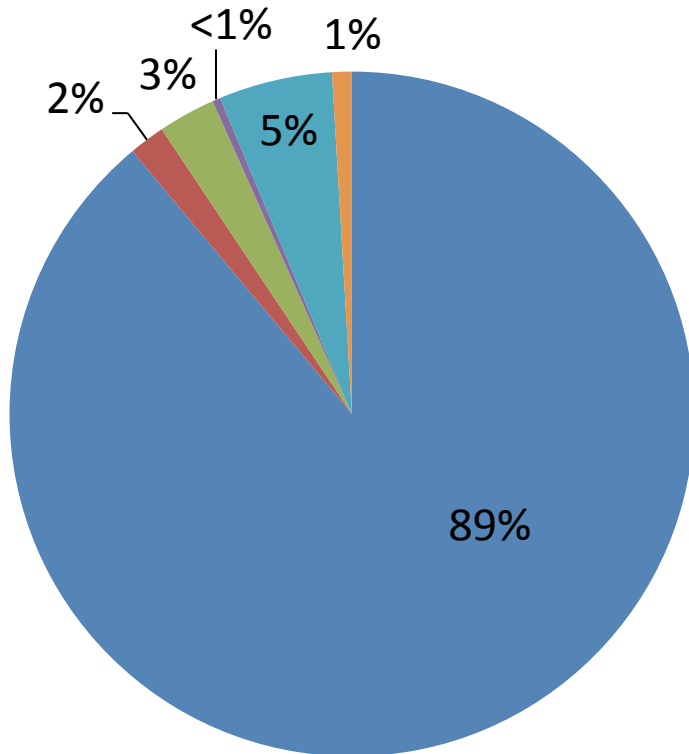


Traffic Volume, No Outliers

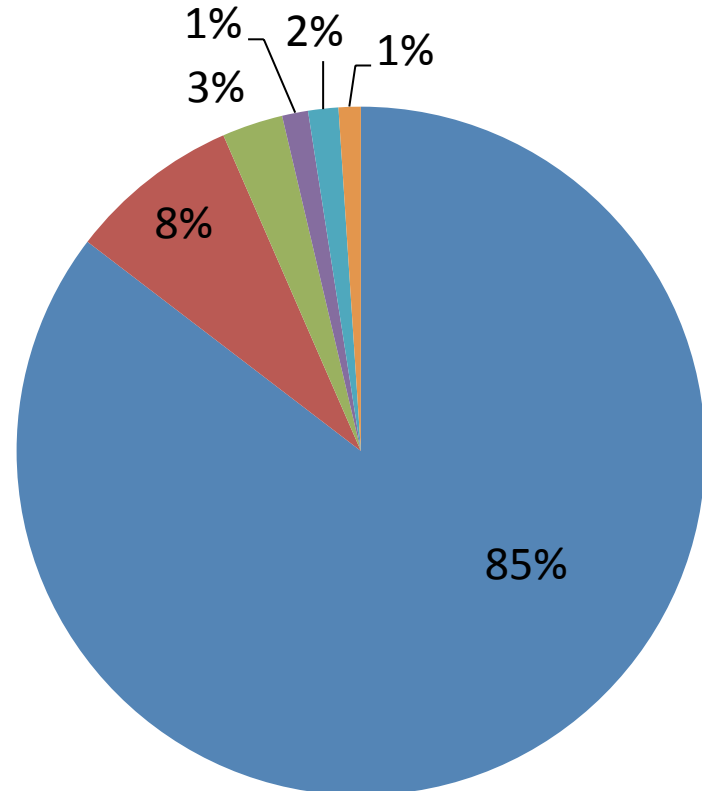


OS Statistics

Bitsquats

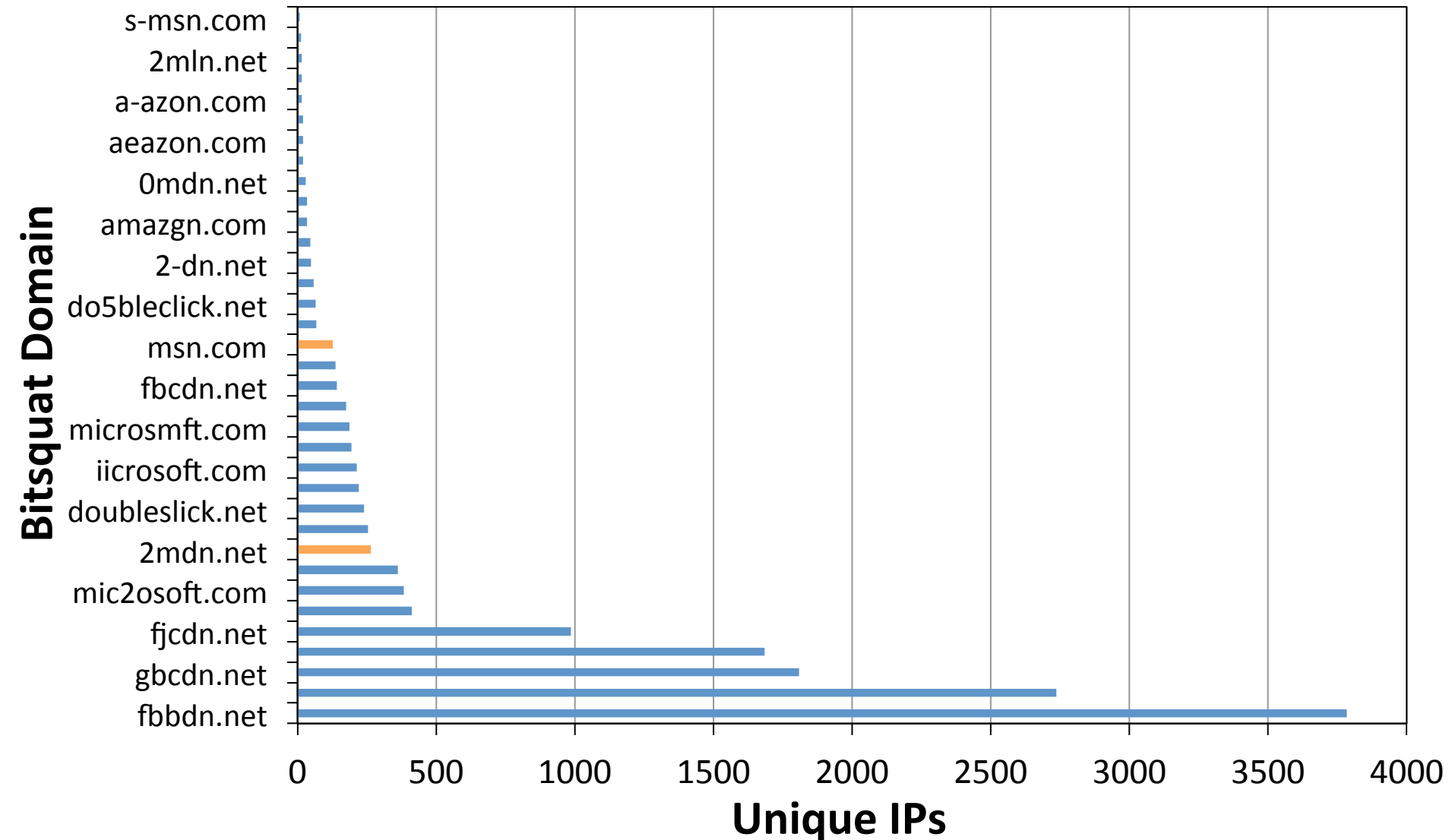


Wikipedia



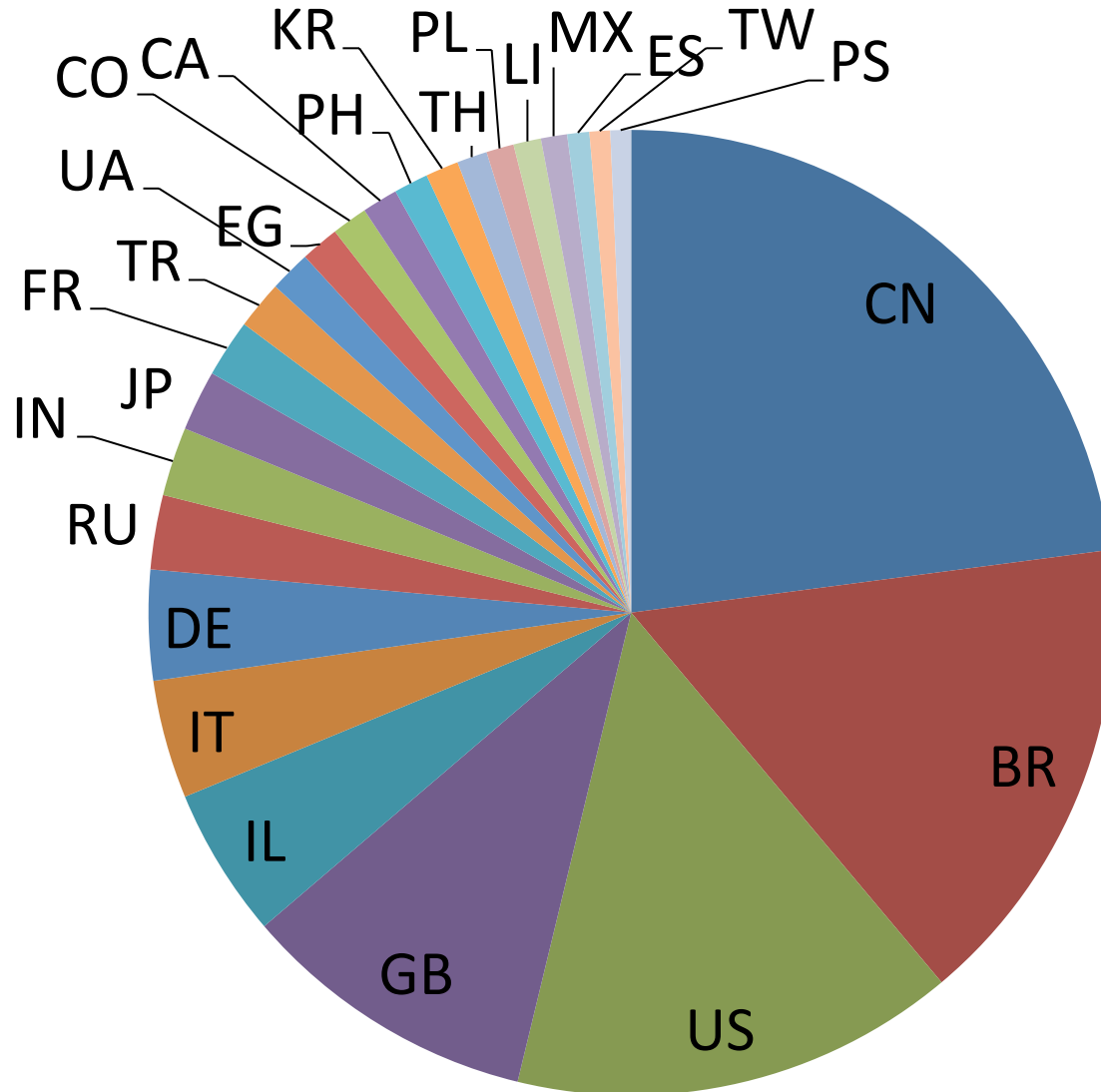
Windows Mac iPhone Linux Other Android

Bitsquat Popularity

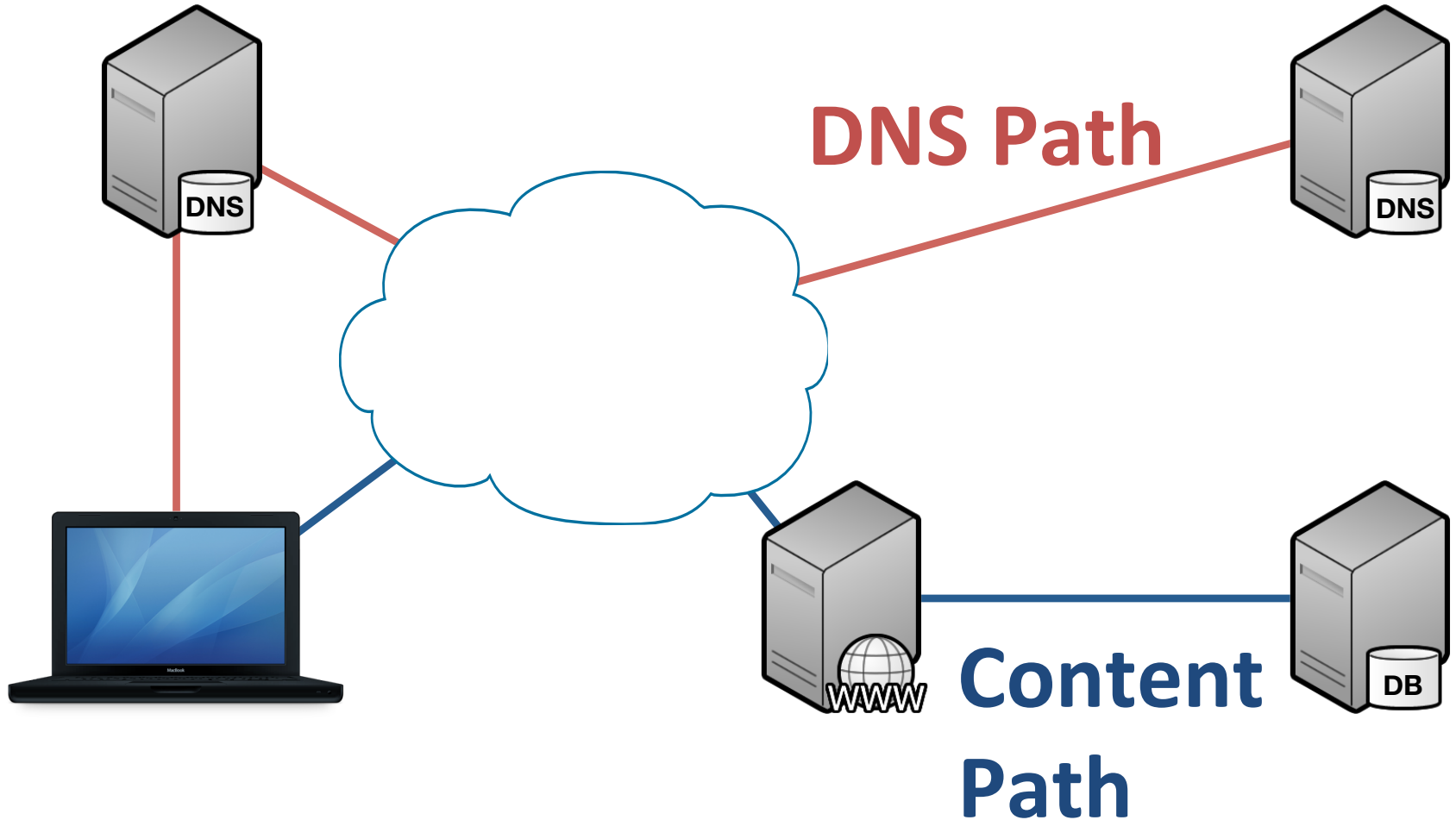


Visitors by Country

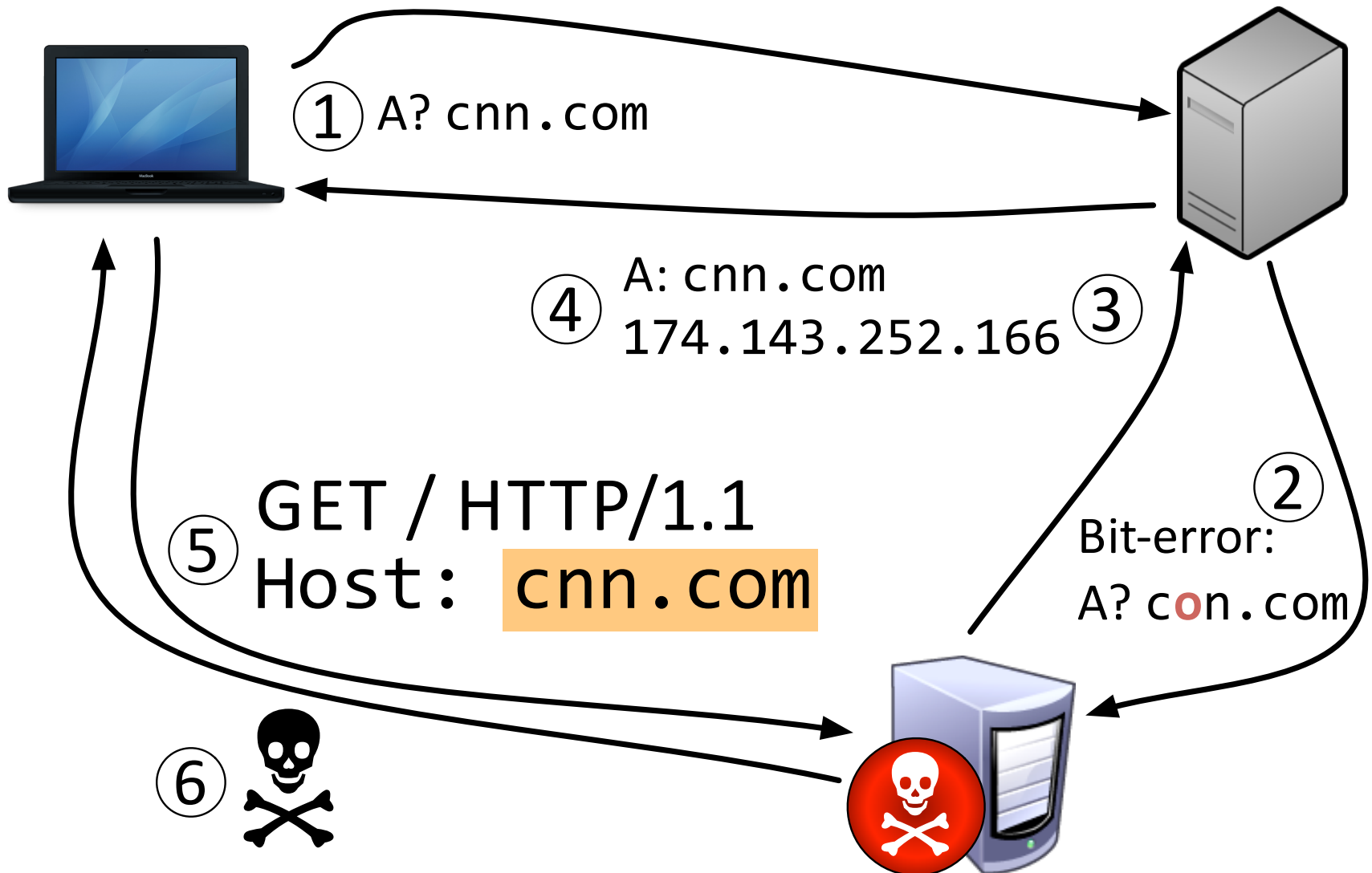
(bitsquats of microsoft.com)



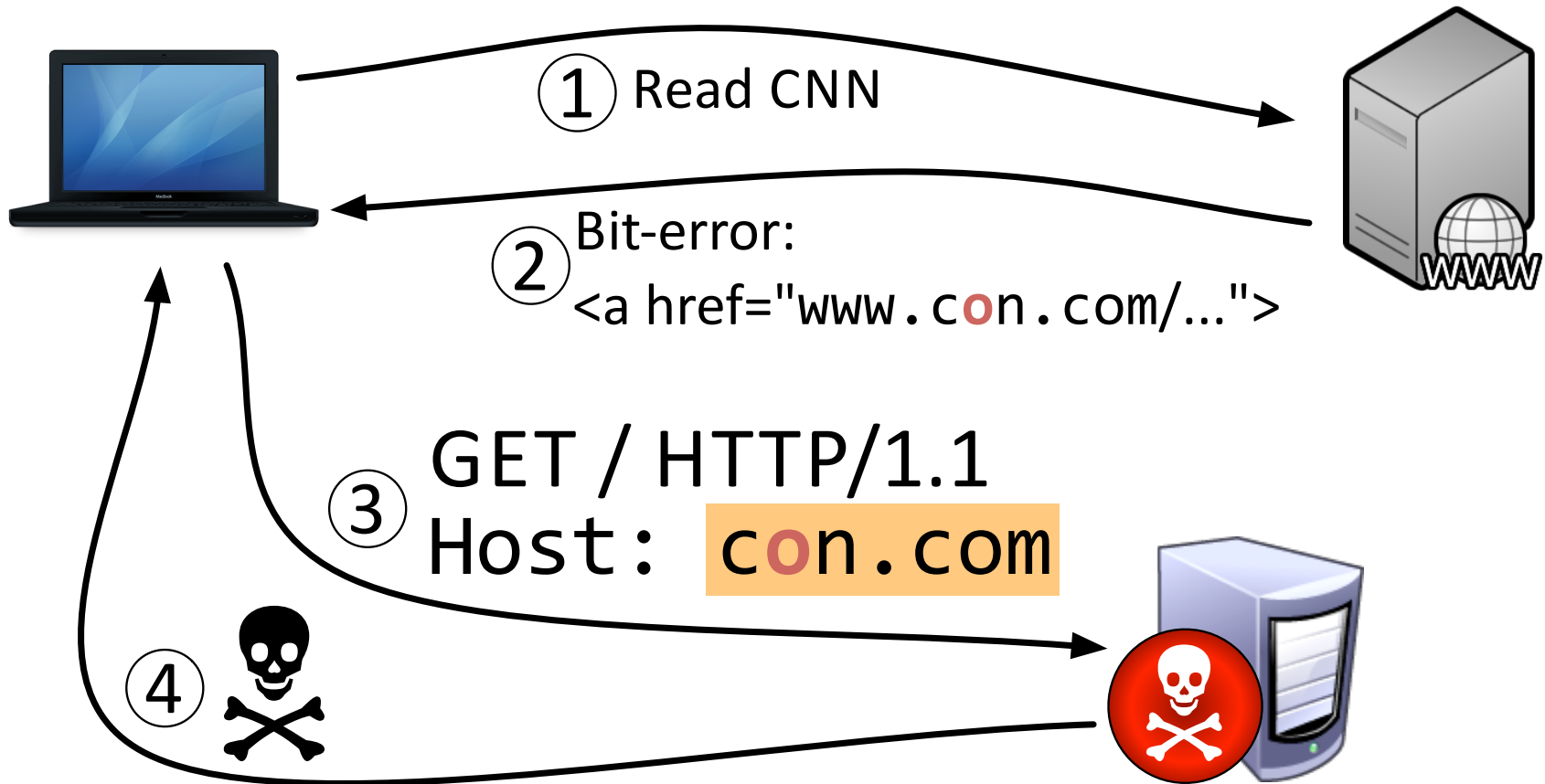
Where Bit-errors Happen



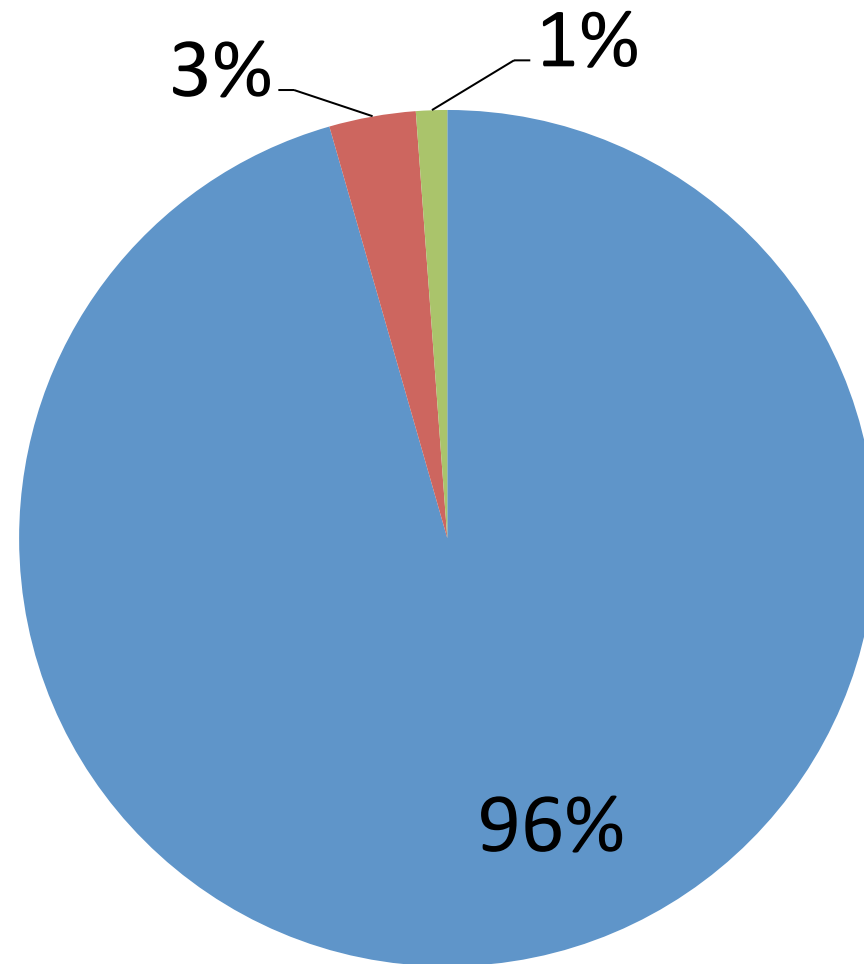
Bit-errors on the DNS Path



Bit-errors on the Content Path



Domain in HTTP Host Header



Bitsquat

Original

Other

Real Example: Other Domains

ax.init.itunes.apple.com 81.225.40.xxx "GET /WebObjects/MZInit.woa/wa/initiateSession?ix=2 HTTP/1.1" 404 202 "-" "iTunes-iPhone/4.1 (4; 16GB)"
mmv.admob.com 109.175.185.xxx "GET /static/iphone/img/app@2x.png HTTP/1.1"
"Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_1 like Mac OS X; HW iPhone2,1; en_gb)
AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-20101108; iphones4.2)"

lifestyle.msn.com 70.91.78.xxx "GET /article_toolbar_your_home.aspx HTTP/1.1"
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6.6; (R1 1.5); .NET CLR
1.0.3705; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .NET
CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

emea.rel.msn.com 194.50.104.xxx "GET /default.aspx?
di=10230&pi=95517&ps=33229&pageid=8522097&mk=ru-ru&tp=http%3A%2F%2Fru.
msn.com%2F&fk=default&gp=S&optkey=default&parsergroup=hops HTTP/1.1" 404
184 "http://ru.msn.com/?ocid=iehp" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT
5.1; .NET CLR 2.0.50727; .NET4.0C; .NET4.0E; .NET CLR 3.0.4506.2152; .NET CLR
3.5.30729)"

Real Examples: Facebook

static.ak.fjcdn.net 109.242.50.xxx "GET /rsrc.php/z67NS/hash/4ys0envq.js HTTP/1.1"
"http://www.facebook.com/profile.php?id=xxxxxxxxxx" "Mozilla/4.0 (compatible;
MSIE 8.0; Windows NT 6.0; WOW64; Trident/4.0; GTB6.5; SLCC1; .NET CLR 2.0.50727;
Media Center PC 5.0; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.2; Hotbar
11.0.78.0; OfficeLiveConnector.1.5; OfficeLivePatch.1.3; AskTbZTV/5.8.0.12304)"

b.static.ak.dbccdn.net 122.168.204.xxx "GET /rsrc.php/zk/r/70eOUKPXS_5.js HTTP/1.1"
"http://www.facebook.com/home.php?sk=lf" "Mozilla/4.0 (compatible; MSIE 8.0;
Windows NT 5.1; Trident/4.0)"

static.ak.fbcdn.net 194.98.30.xxx "GET /rsrc.php/yq/r/ypBeM1b0IFS.js HTTP/1.1"
"http://m.facebook.com/home.php?refsrc=m.facebook.com
%2Fid02.qnitabxn.site.prn.miyowa.net%2FSD2q10oklmcvyqv0v45s1zz4z452DS
%2Fhome.aspx&refid=7&m_sess=soz7CzQ1-lOioUPsT&_rdr" "Mozilla/5.0 (Linux; U;
Android 2.1-update1; fr-fr; GT-I5800 Build/ECLAIR) AppleWebKit/530.17 (KHTML, like
Gecko) Version/4.0 Mobile Safari/530.17"

Real Examples: Windows Update

download.microsoft.com 91.198.175.xxx "GET /v9/windowsupdate/redir/muv4wuredir.cab?1010161718 HTTP/1.1" "Windows-Update-Agent"

www.update.microsoft.com 201.144.5.xxx "HEAD /v9/windowsupdate/selfupdate/wuident.cab?1011010912 HTTP/1.1" "Windows-Update-Agent"

beta.update.microsoft.com 113.117.249.xxx "GET /microsoftupdate/v6/default.aspx?1290162381 HTTP/1.1" "http://beta.update.microsoft.com/microsoftupdate/v6/default.aspx" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; GTB6.6; SLCC1; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30618)"

download.microsoft.com 91.13.83.xxx "HEAD /WM/MicrosoftUpdate/redir/duredir.cab HTTP/1.1" "Windows-Mobile-Device-Update-Agent"

msgr.dlservice.microsoft.com 213.178.224.xxx "GET /download/A/6/1/A616CCD4-B0CA-4A3D-B975-3EDB38081B38/ar/wlsetup-cvr.exe HTTP/1.1" 404 268 "-"
"Microsoft BITS/6.6"

Real Examples: Webmail

sn110w.snt110.mail.li6e.com 187.92.218.xxx "GET /mail/clear.gif HTTP/1.1" "http://sn110w.snt110.mail.live.com/mail/InboxLight.aspx?FolderID=00000000-0000-0000-0000-000000000001&n=xxxxxxxx" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; GTB6.5; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

secure.s%28ared.li6e.com 190.95.125.xxx "GET /_/F\$Live.SiteContent.Messenger/4.2.57151/Messenger.html HTTP/1.1" 404 215 "http://bl145w.blu145.mail.live.com/default.aspx?wa=wsignin1.0" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.3 (KHTML, like Gecko) Chrome/6.0.472.63 Safari/534.3"

s0.2l|dn.net 66.82.9.xxx "GET /879366/flashwrite_1_2.js HTTP/1.1" "http://webmail.satx.rr.com/_uac/adpage.html" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; HPNTDF; AskTB5.2)"

Real Examples: Crash Reports

watson.microsnft.com 115.143.103.xxx "GET /StageOne/acrord32_exe/9_3_3_177/
msvcr80_dll/8_0_50727_3053/00008aa0.htm?
OS=5.1.2600.2.00010100.3.0&lcid=1042 HTTP/1.1" "MSDW"

watson.microsnft.com 187.73.247.xxx "GET /StageOne/notepad_exe/
5_1_2600_5512/uxtheme_dll/6_0_2900_5512/00004b43.htm?
OS=5.1.2600.2.00010100.3.0&lcid=1046 HTTP/1.1" "MSDW"

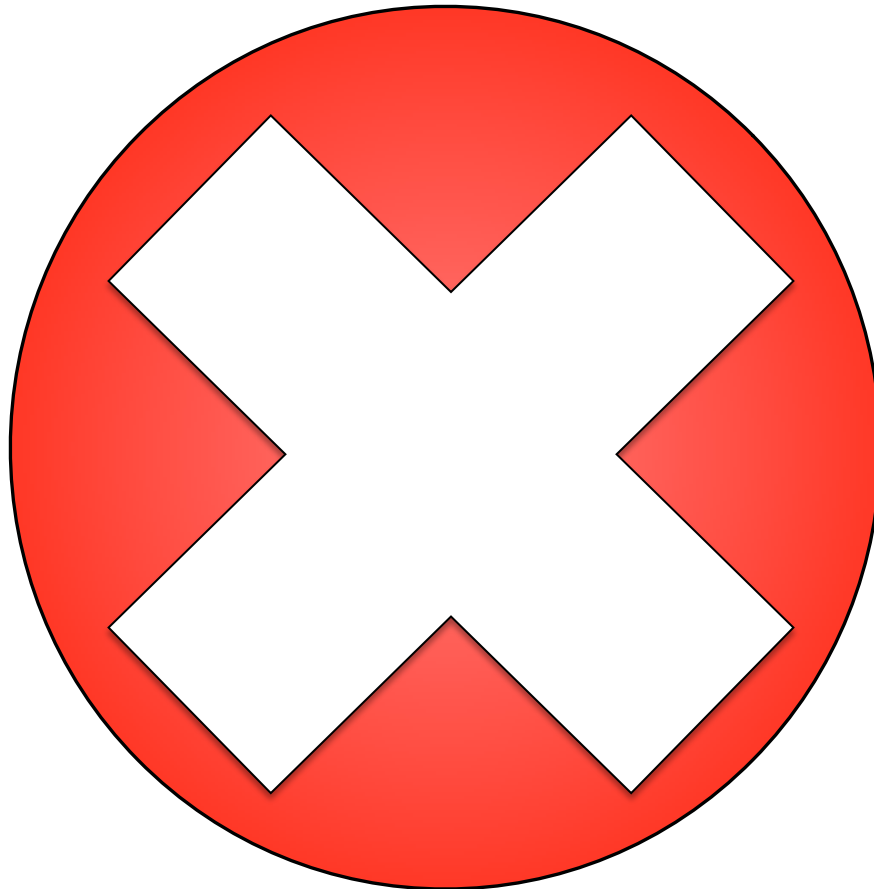
watson.mic2osoft.com 202.156.10.xxx "GET /StageOne/Generic/FaultTolerantHeap/
SearchIndexer_exe/7_0_7600_16385/4A5BD212/ffffbaad.htm?
LCID=18441&OS=6.1.7600.2.00010100.0.0.48.16385&SM=System
%20manufacturer&SPN=System%20Product%20Name&BV=1456 HTTP/1.1" "MSDW"

Mitigations

**ECC ON
EVERYTHING**

Mitigations

Pre-Register Domains



Mitigations

Trust

But

your data

Verify

- Ronald Reagan

Special Thanks

Robert Edmonds

Paul Royal

Aaron LeMasters

Raytheon Rosslyn Office

Patient and Supportive Reviewers

BlackHat Staff

Questions?



Image Attribution

- Slide 2: Earth © by NASA
- Slide 3: Logos © their respective owners
- Slide 4: Childrens Blocks © by Flickr User: lobo235
- Slide 5: Dollar bills © by Flickr User: Images_of_Money
- Slide 9: HAL 9000 © Warner Brothers Pictures
- Slide 13: MITS Altair RAM board image © 2005 George M. Phillips Jr.
- Slide 14: Sun UltraSparc II Processor © by Konstantin Lanzet. Wikimedia user: Appaloosa
- Slide 16: Fighting with RAM © by Flickr User: elecnix
- Slide 17: Heat Lamp. “Using memory errors to attack a virtual machine” by Govindavajhala and Appel, IEEE S&P 2003
- Slide 18: Smart Cards © by Hywel Clatworthy. Wikimedia user: Dacs
- Slide 19: Desert Sun © by Flickr User: Steve & Jemma Copley
- Slide 21: Backup Power © by David Robinson. Flickr User: dgrobinson
- Slide 22: Fake Capacitor. Found on Internet, likely from chinauser.cn
- Slide 23: Homunculus Nebula © by NASA
- Slide 25: Mystery Box © by Flickr User: TEDxNJLibraries
- Slide 26: DRAM. Self
- Slide 27: SAS Drive. Self
- Slide 29: BSOD © by Wayne Williamson. Flickr User: ka3vo
- Slide 20: Blue Marble. NASA
- Slide 31: Error at airport. Self.

Please Remember to Complete Your Feedback Form



USA + 2011
EMBEDDING SECURITY