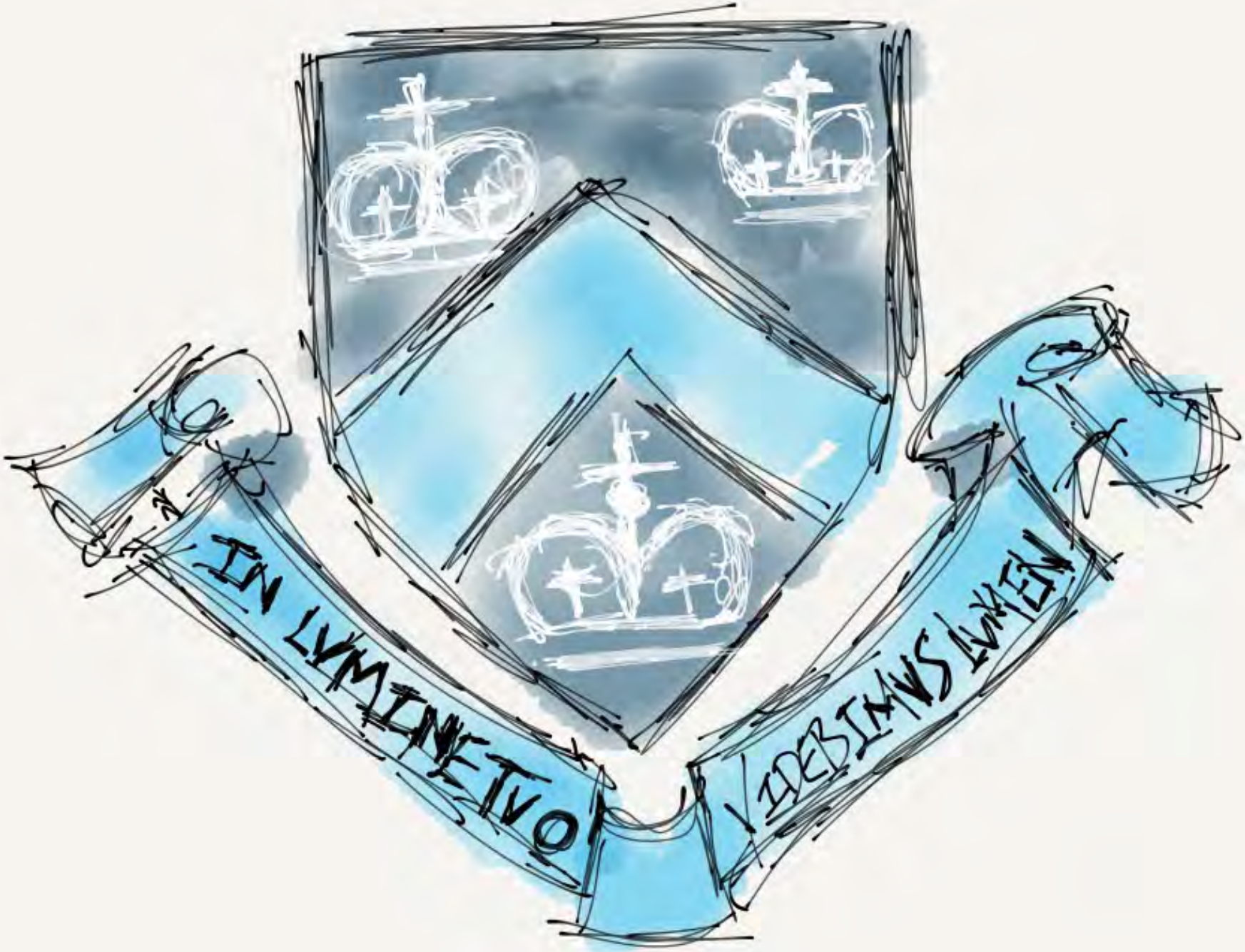
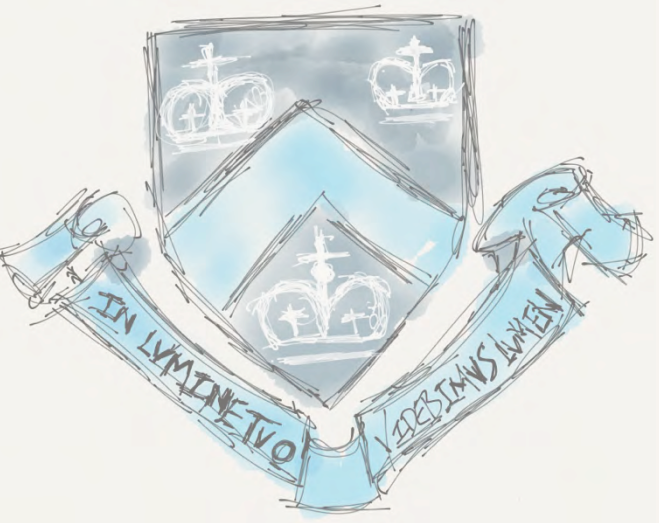

IN LVMINE TVO
VIDEBIMVS LVMEN

When Firmware Modifications ATTACK!

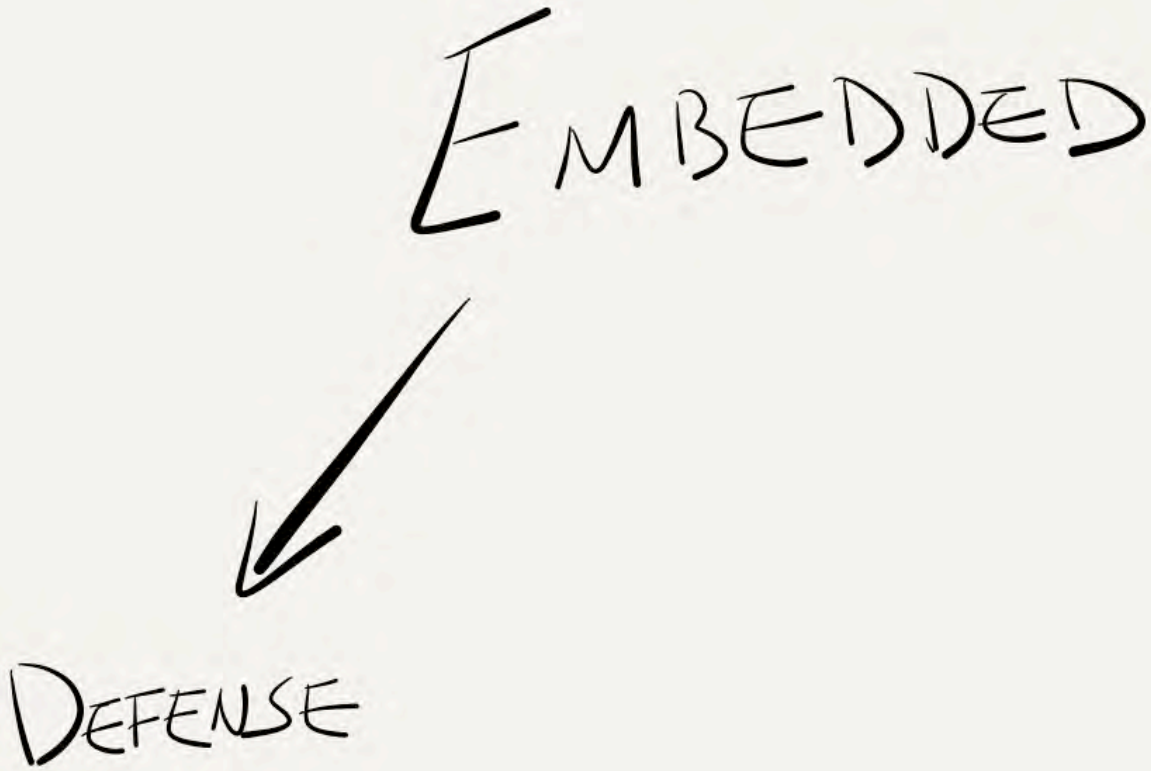


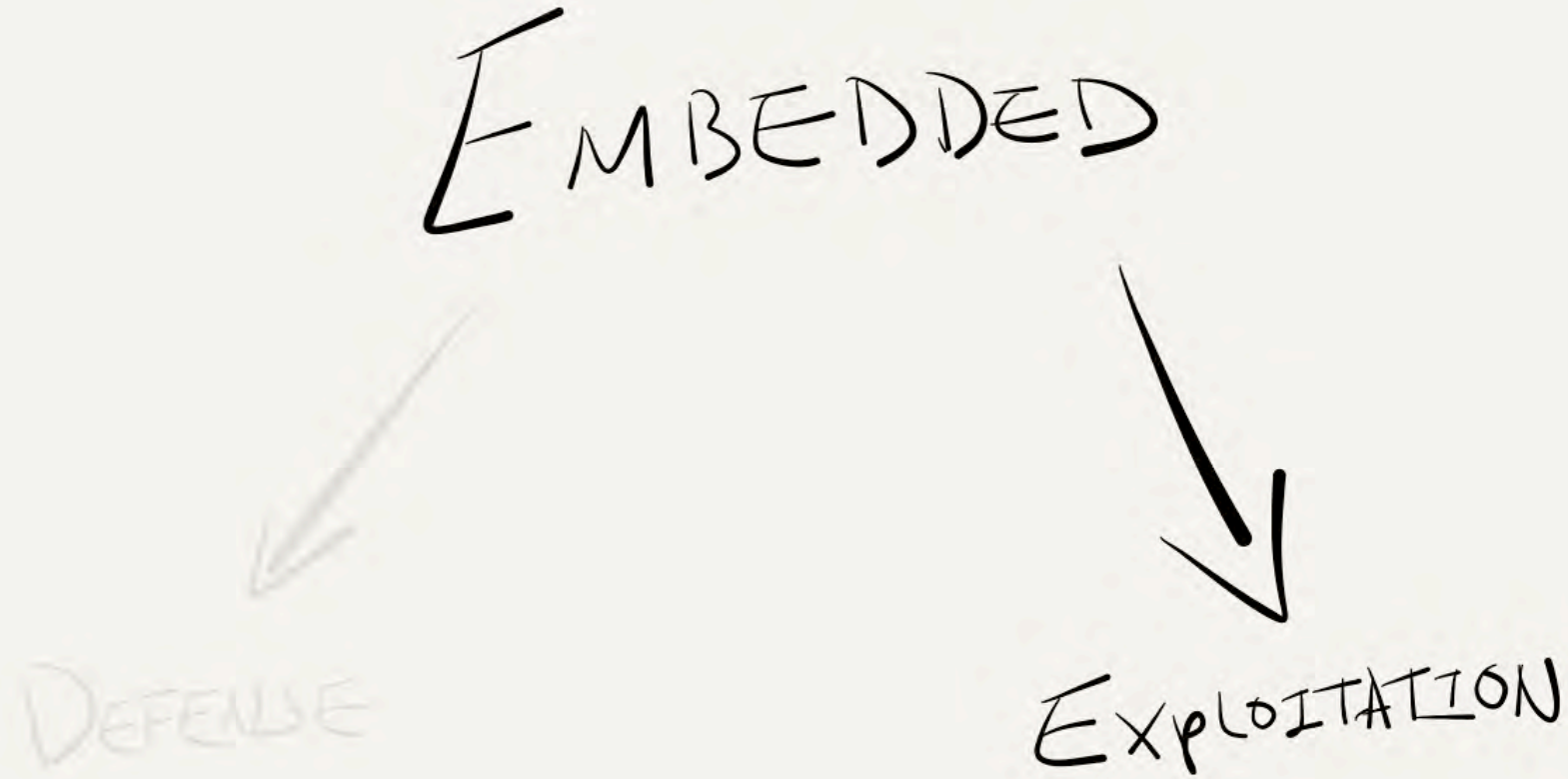
ANG CUI
PHD CANDIDATE COLUMBIA UNIVERSITY

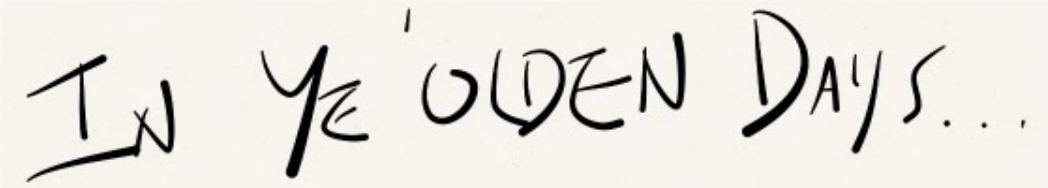
MICHAEL COSTELLO
STAFF RESEARCH SCIENTIST COLUMBIA UNIVERSITY

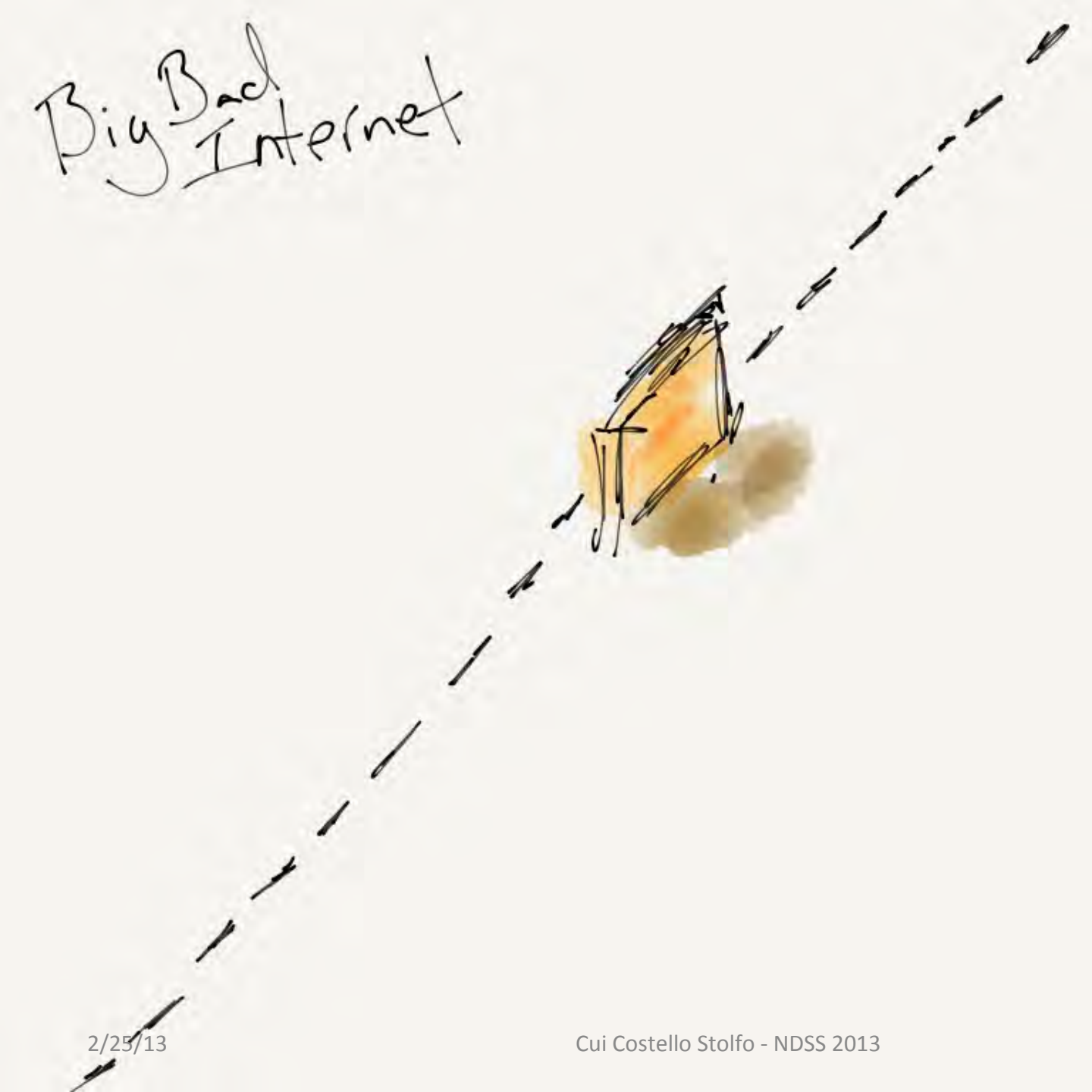
DR. SALVATORE J. STOLFO
PROFESSOR OF COMPUTER SCIENCE COLUMBIA UNIVERSITY

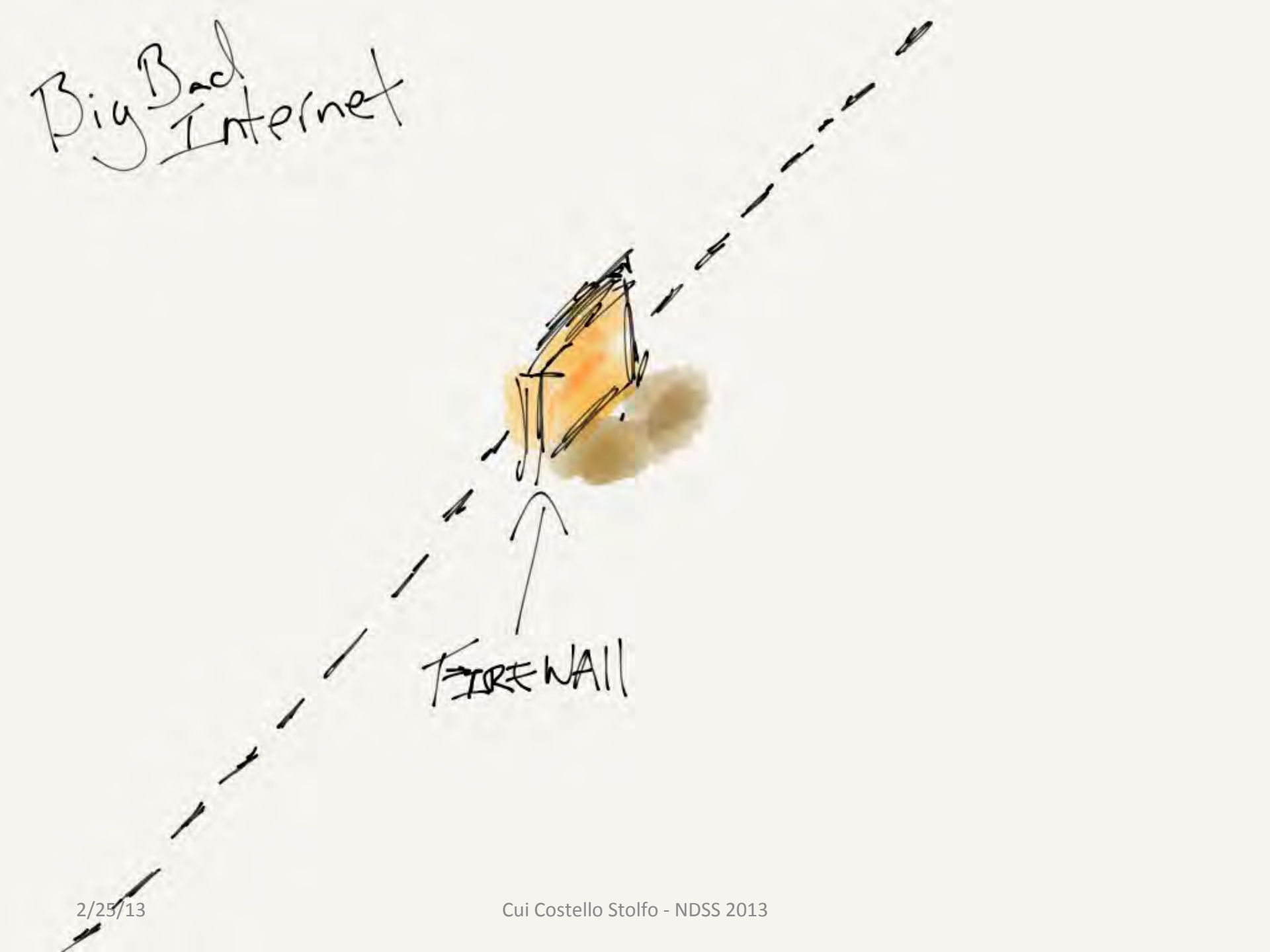

EMBEDDED

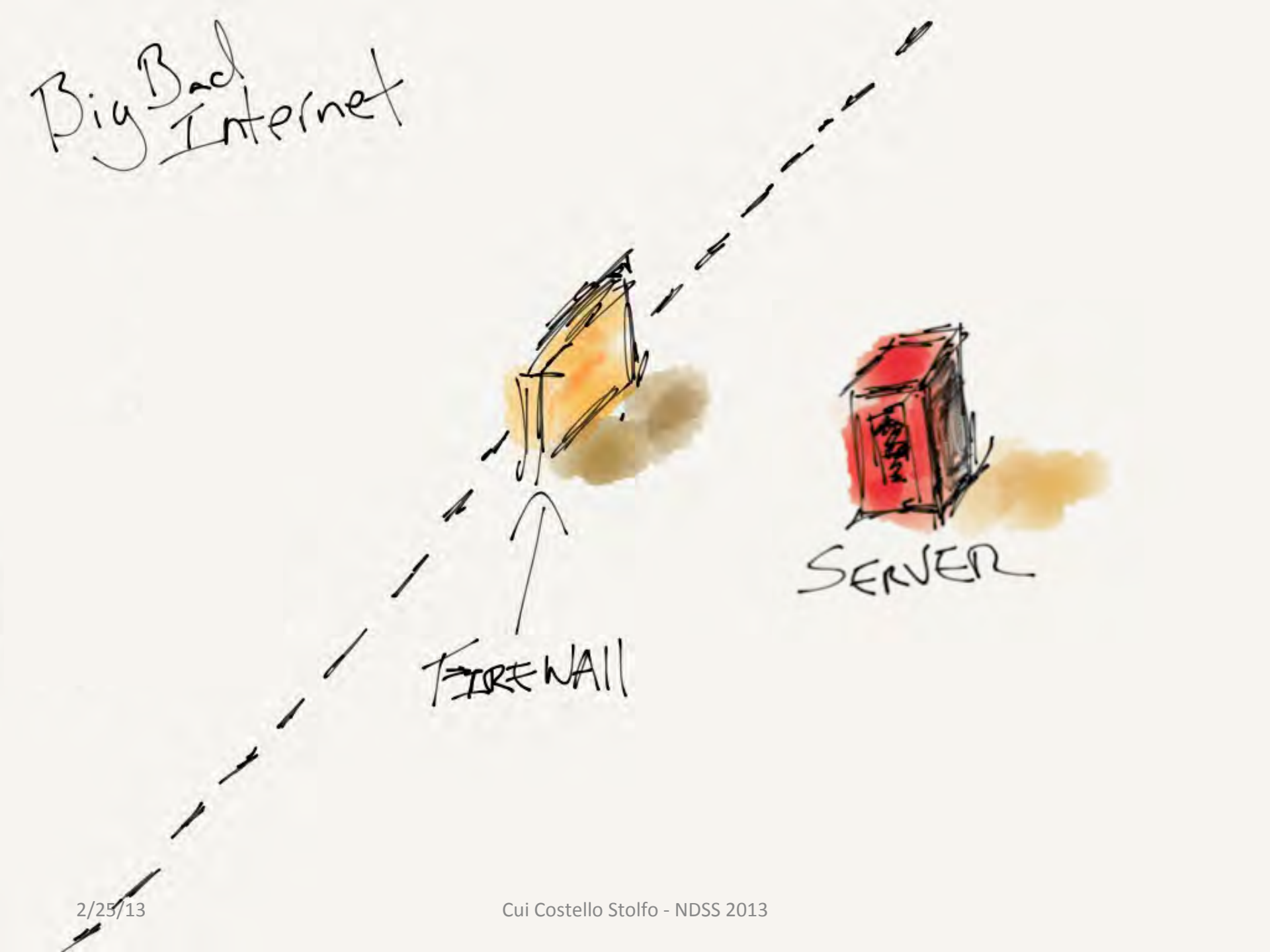

EMBEDDED
DEFENSE

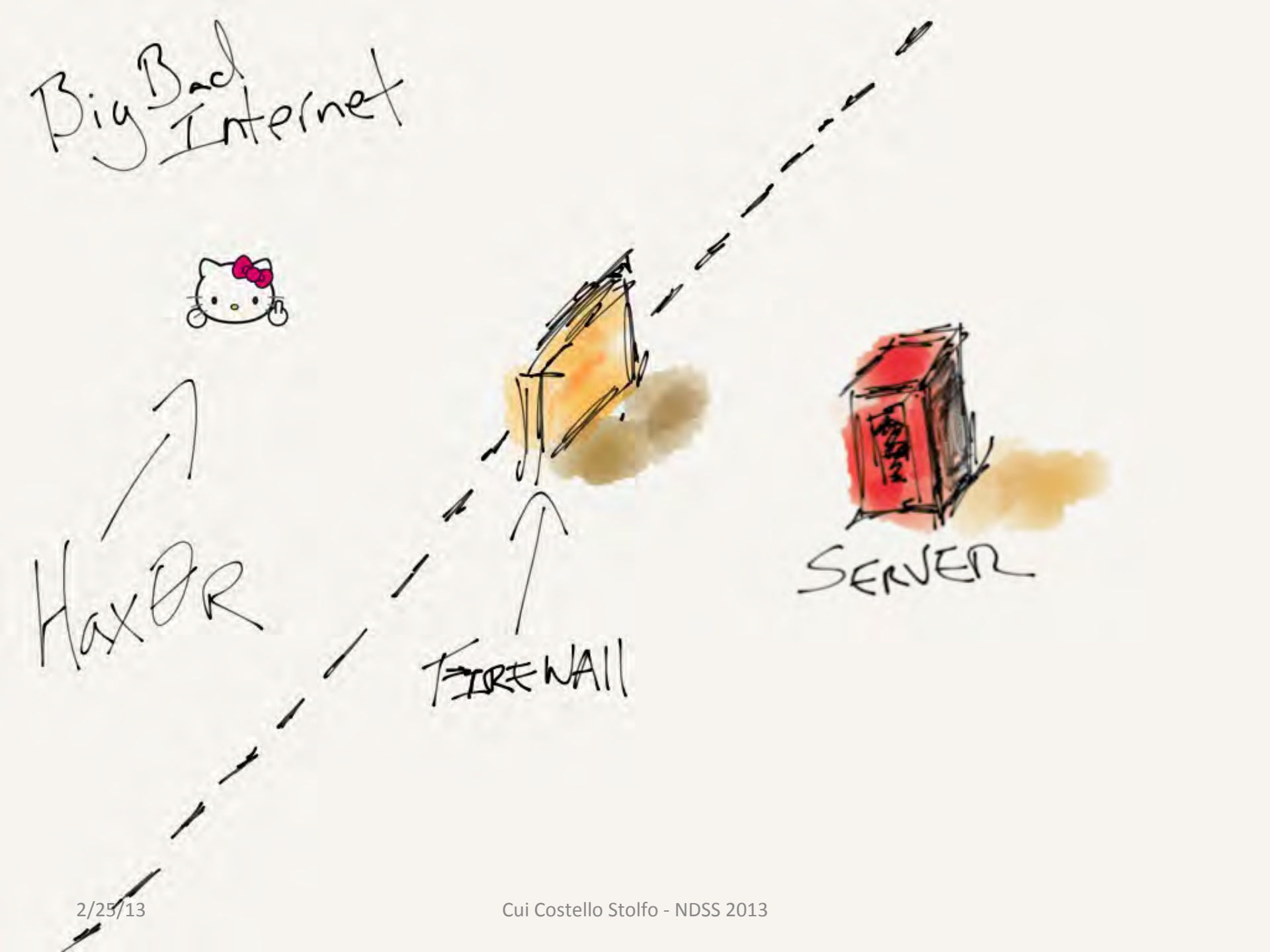

EMBEDDED
DEFENSE
EXPLOITATION

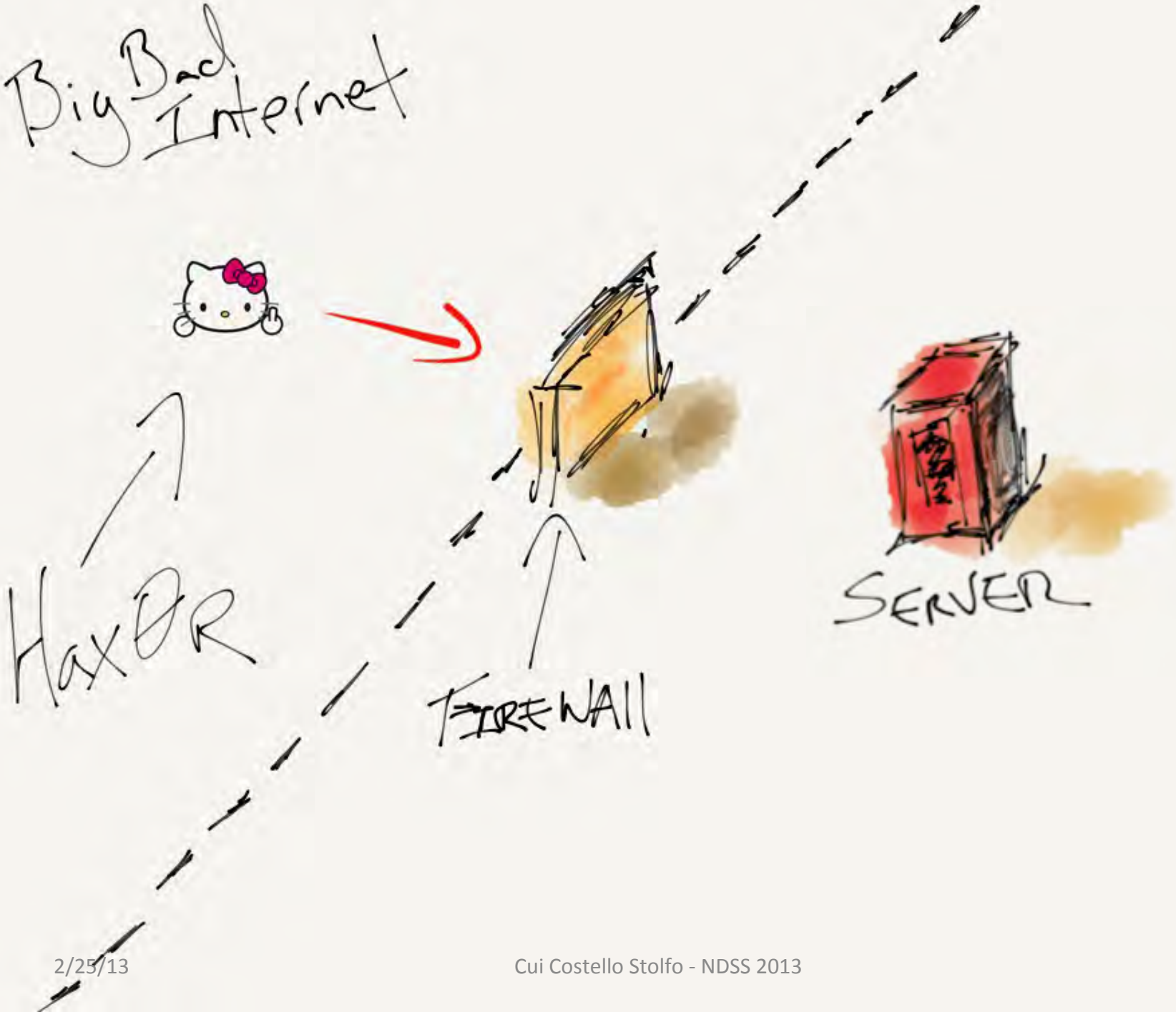

In Ye 'olden Days...

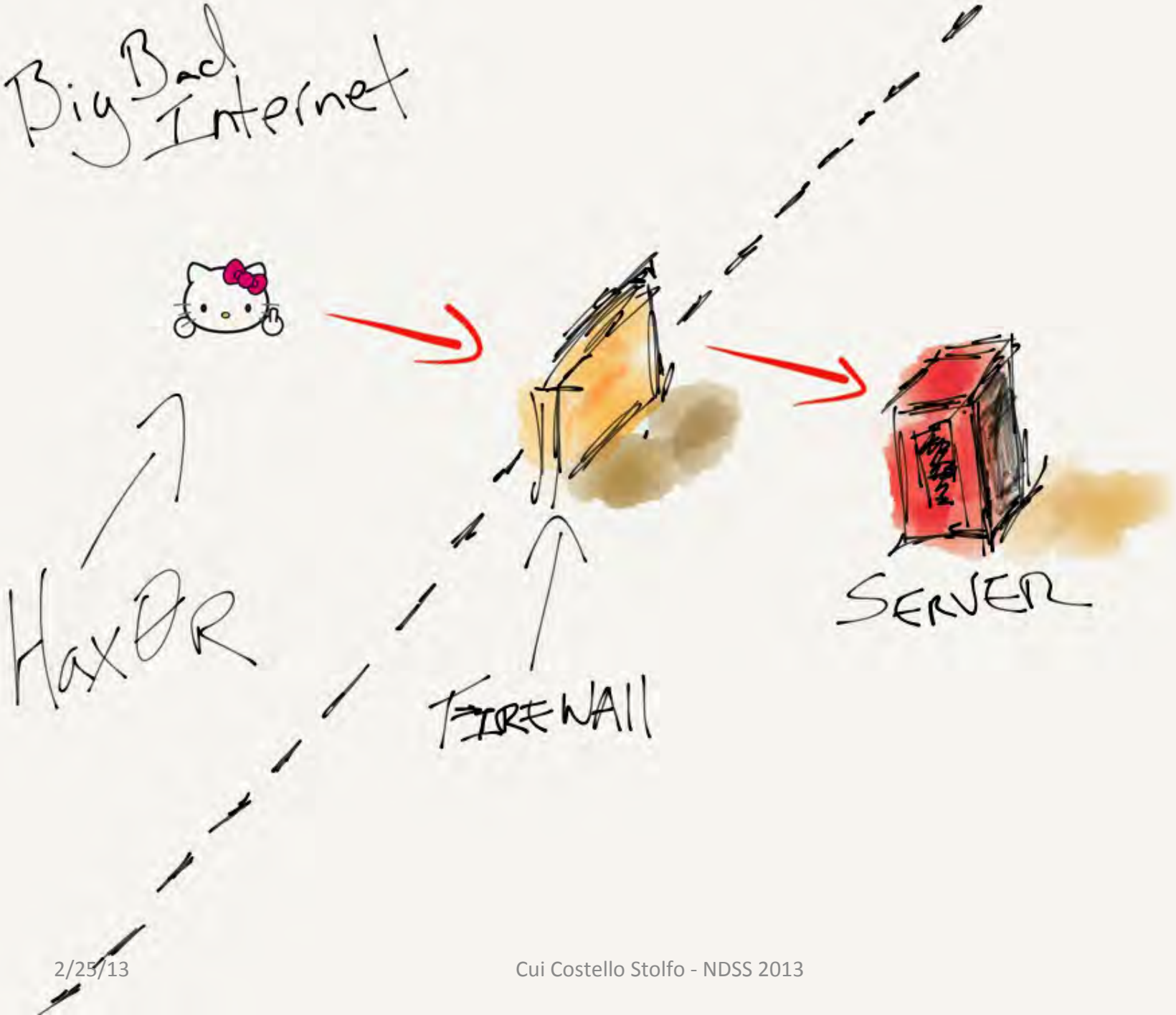

Big Bad Internet

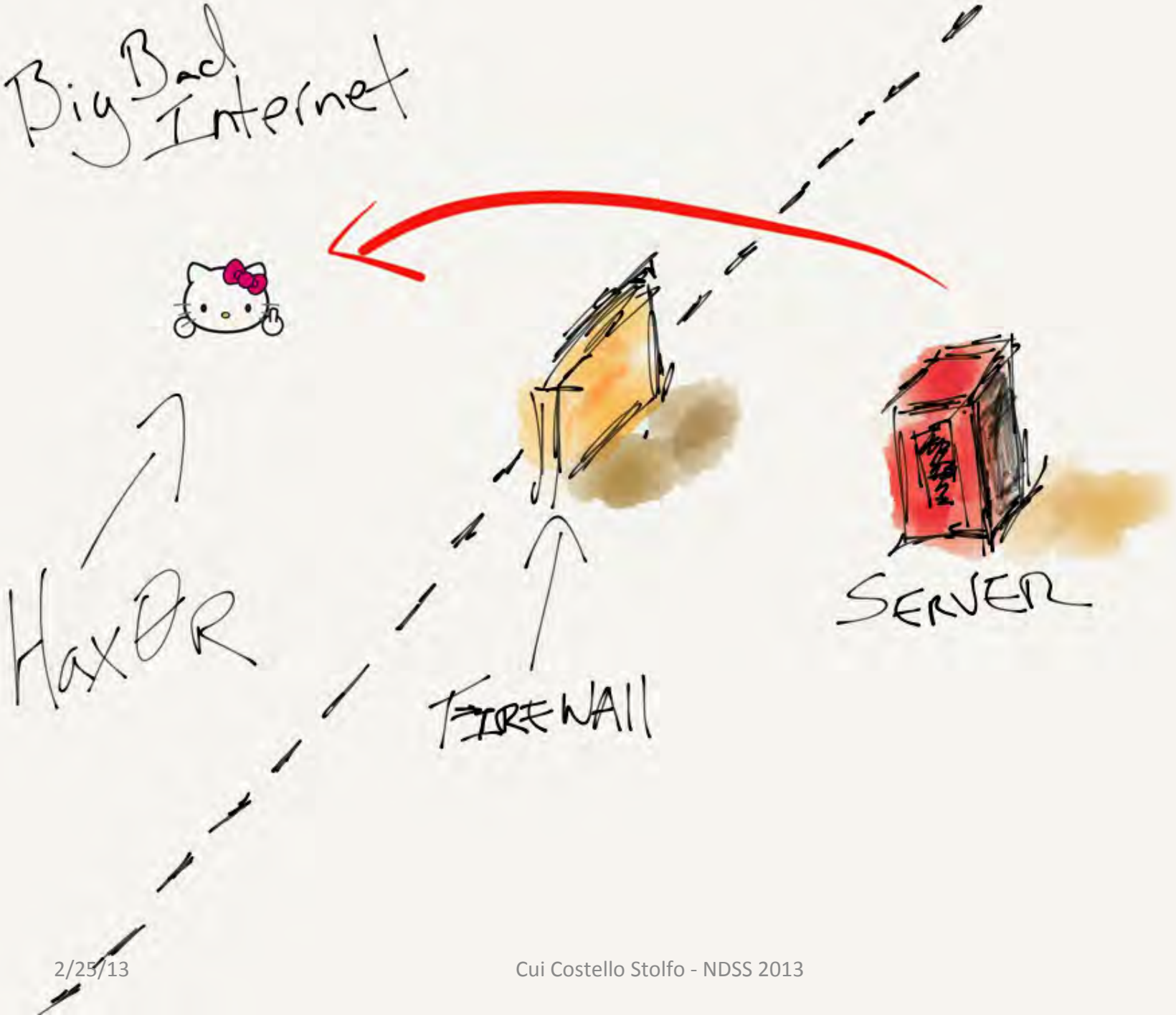

Big Bad Internet
FIREWALL

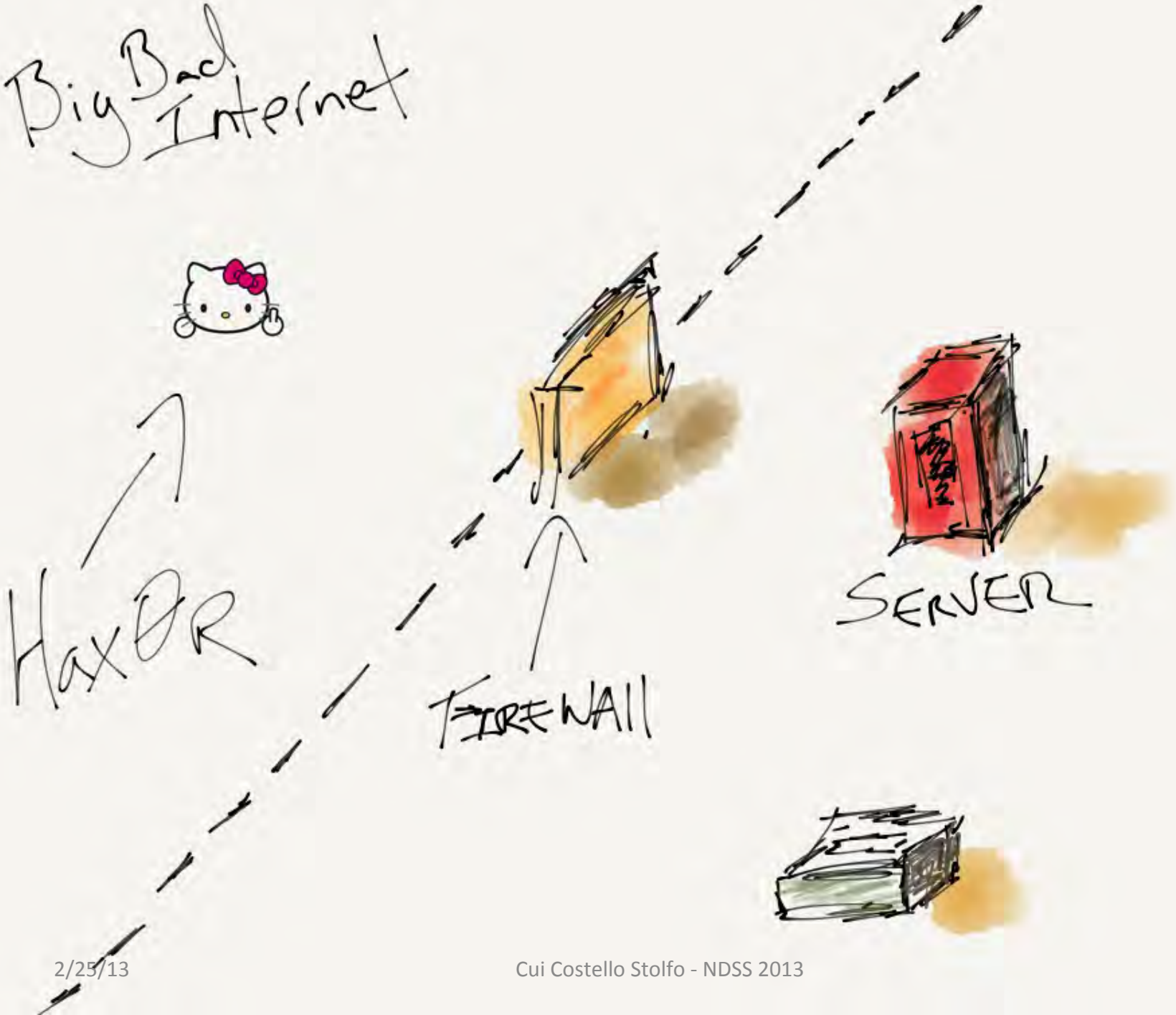

Big Bad Internet
FIREWALL
SERVER

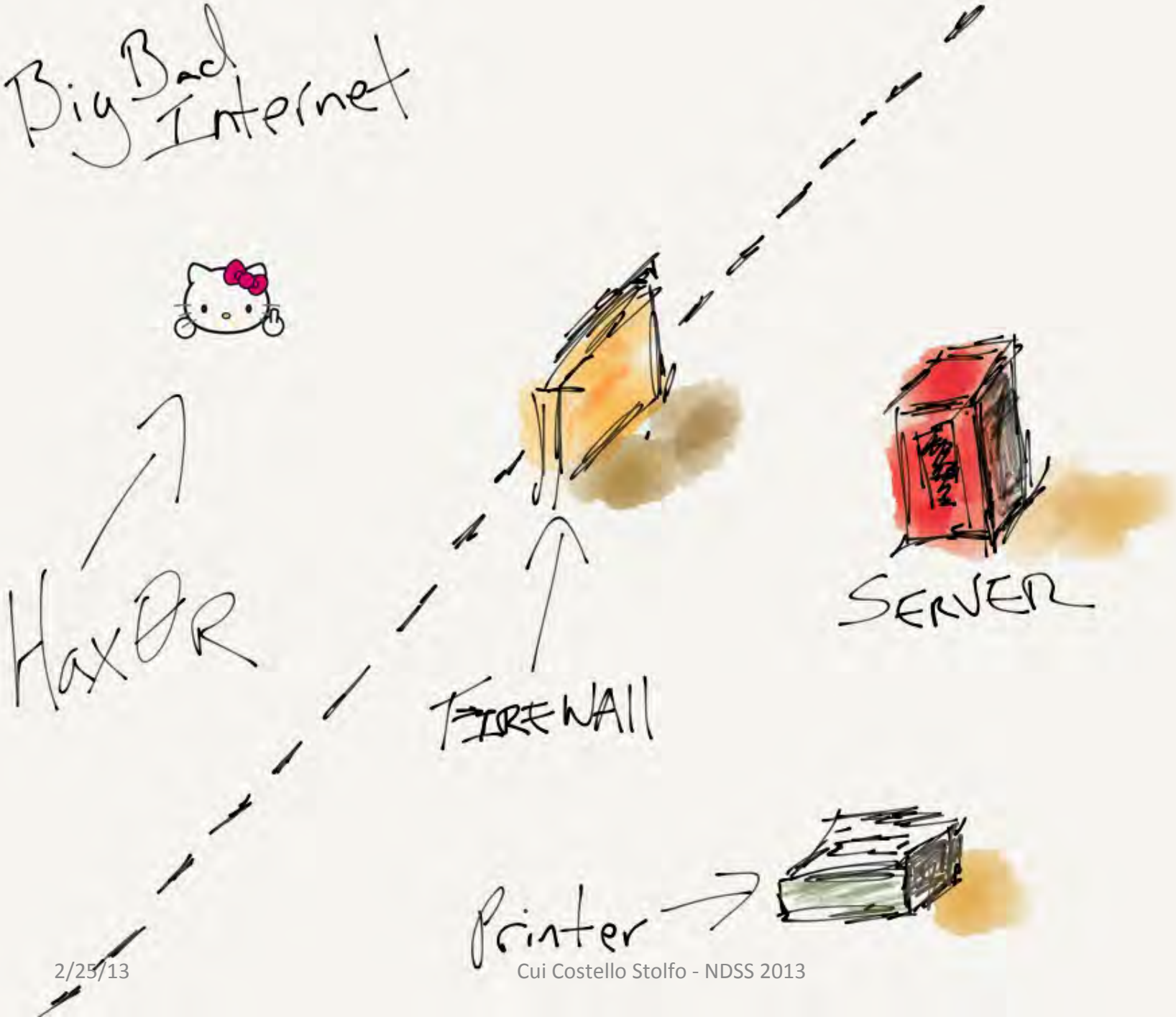

Big Bad Internet
HaxOR
FIREWALL
SERVER

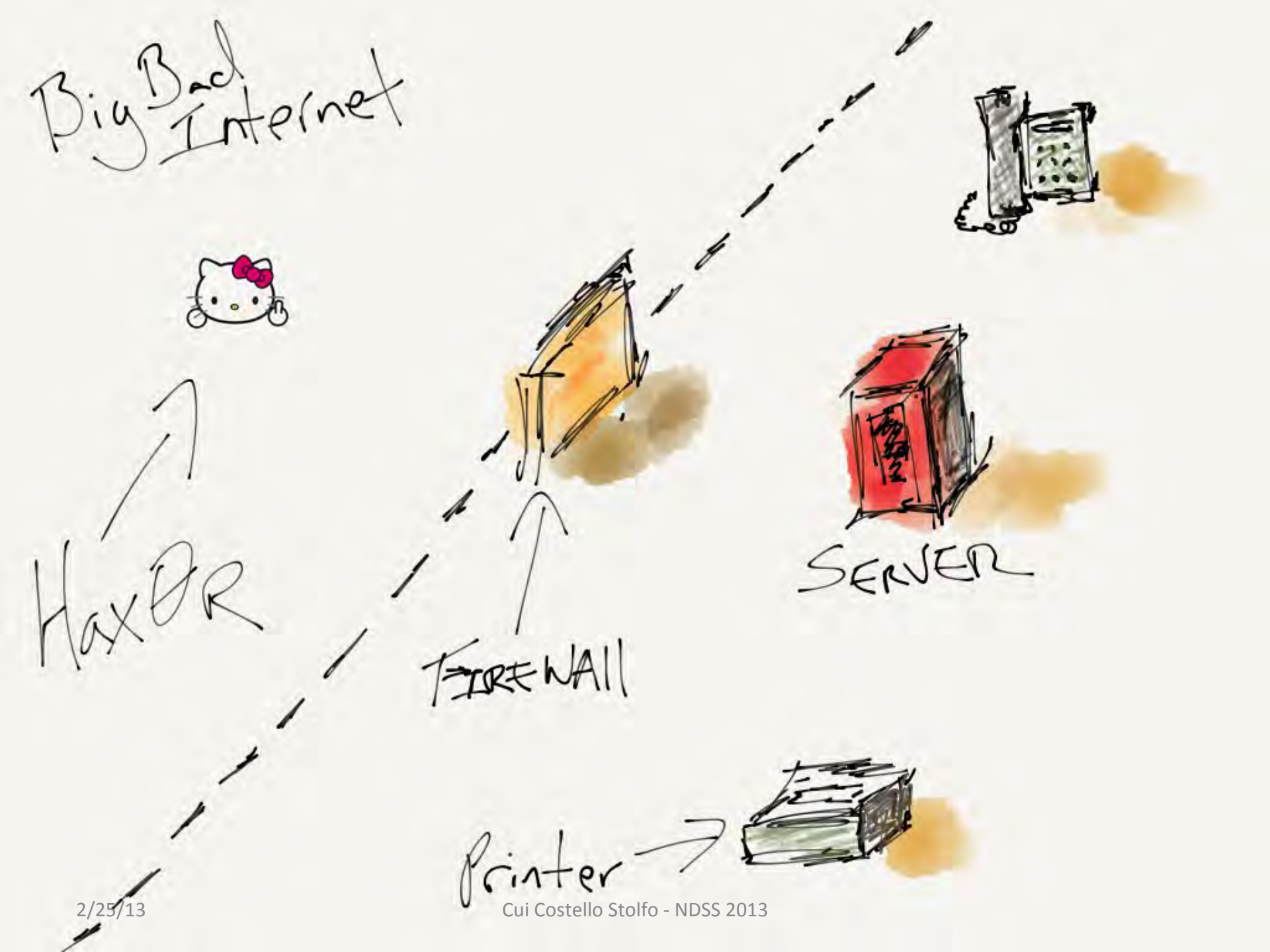

Big Bad Internet
HaxOR
FIREWALL
SERVER

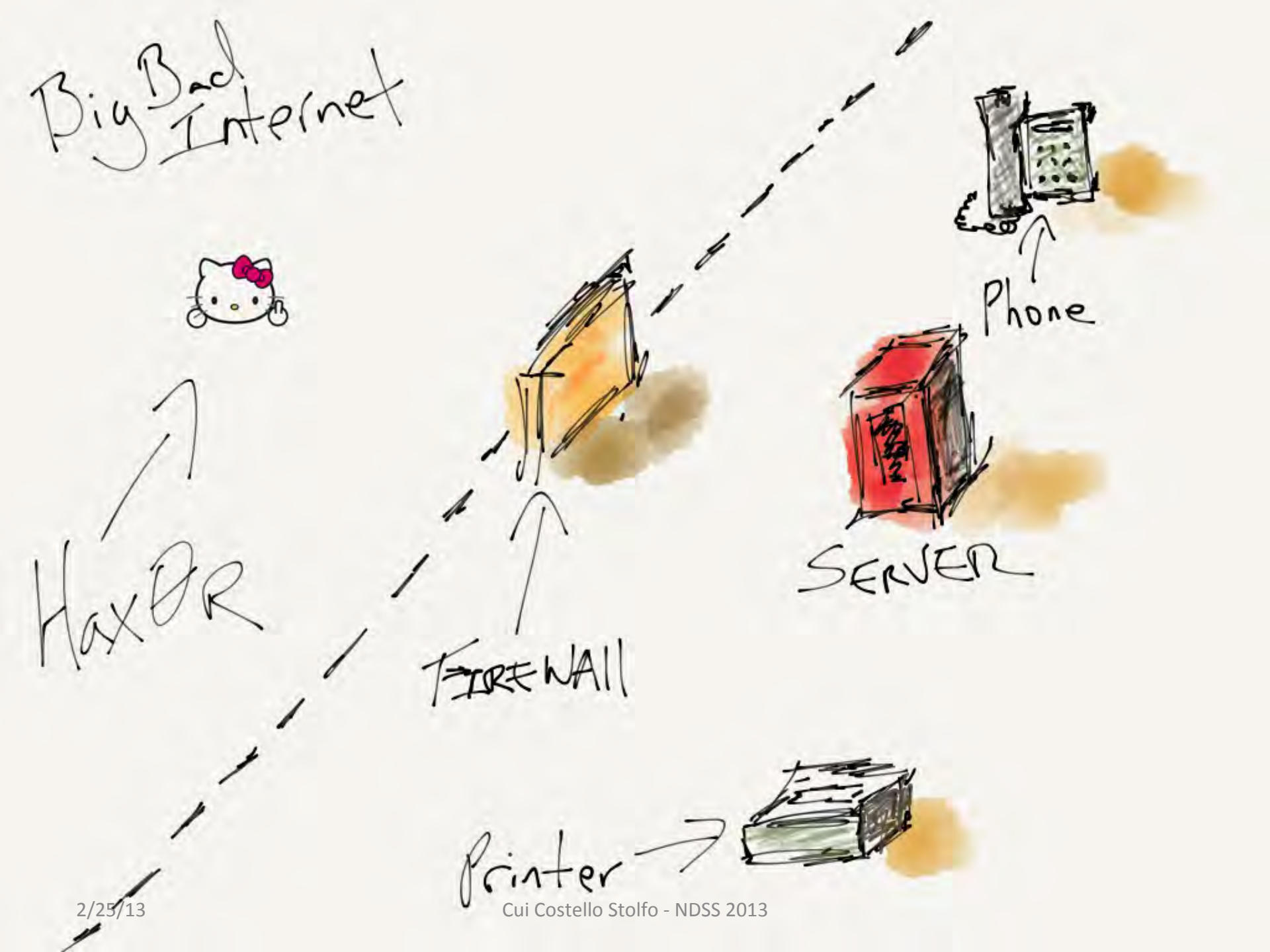

Big Bad Internet
HaxOR
FIREWALL
SERVER


Big Bad Internet
HaxOR
FIREWALL
SERVER

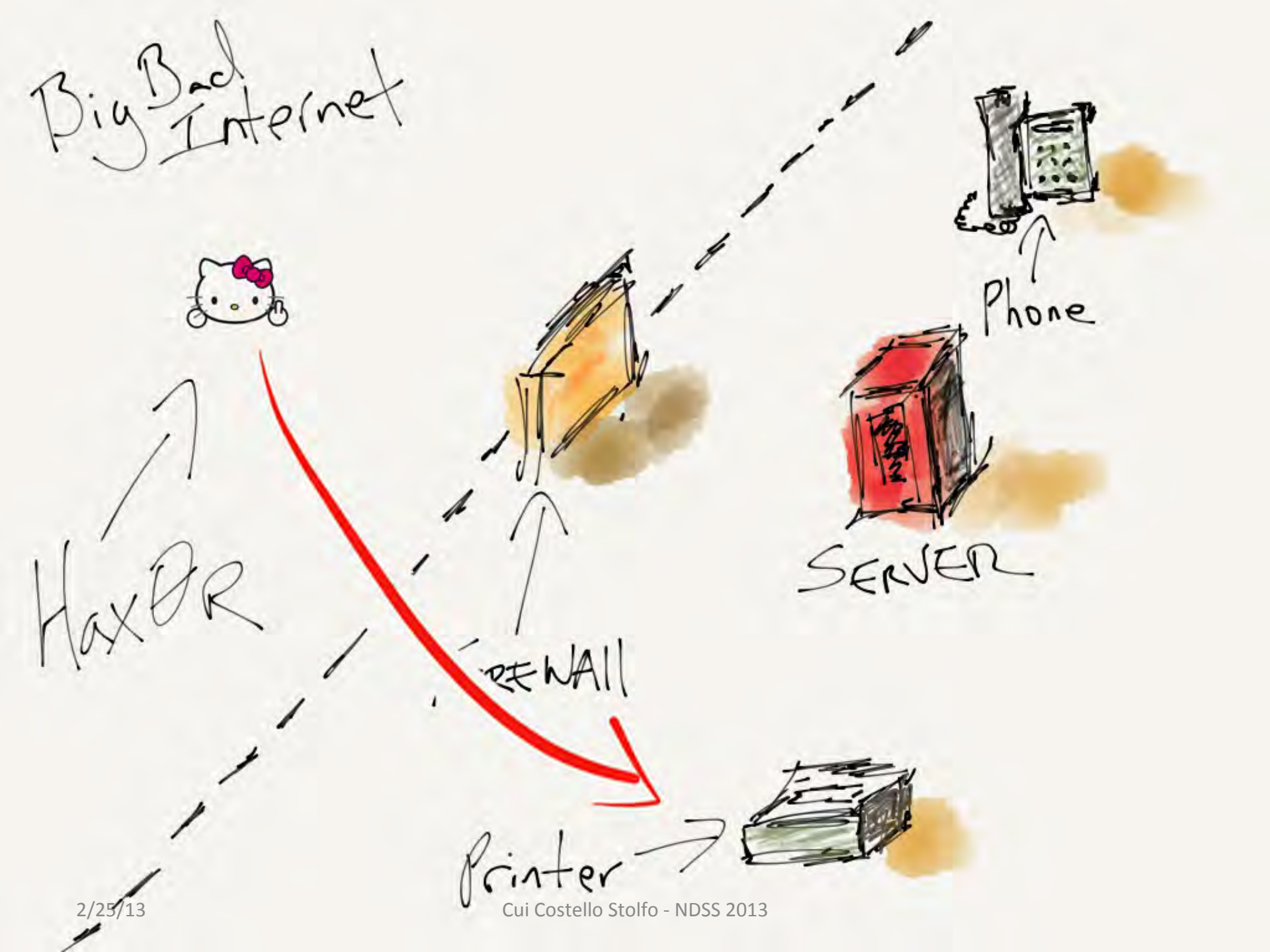

Big Bad Internet
HaxOR
FIREWALL
SERVER

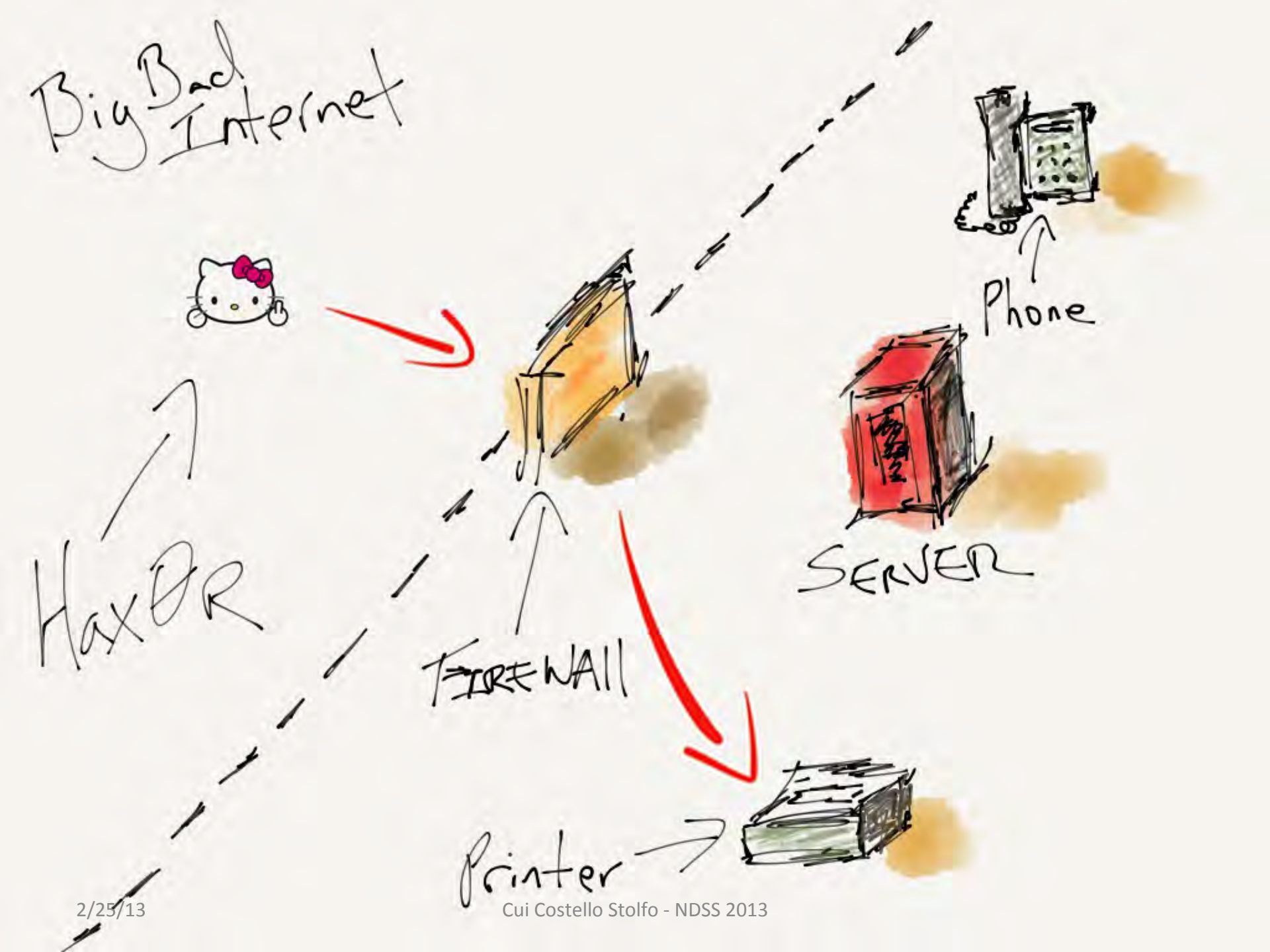

Big Bad Internet
HaxOR
FIREWALL
SERVER
Printer

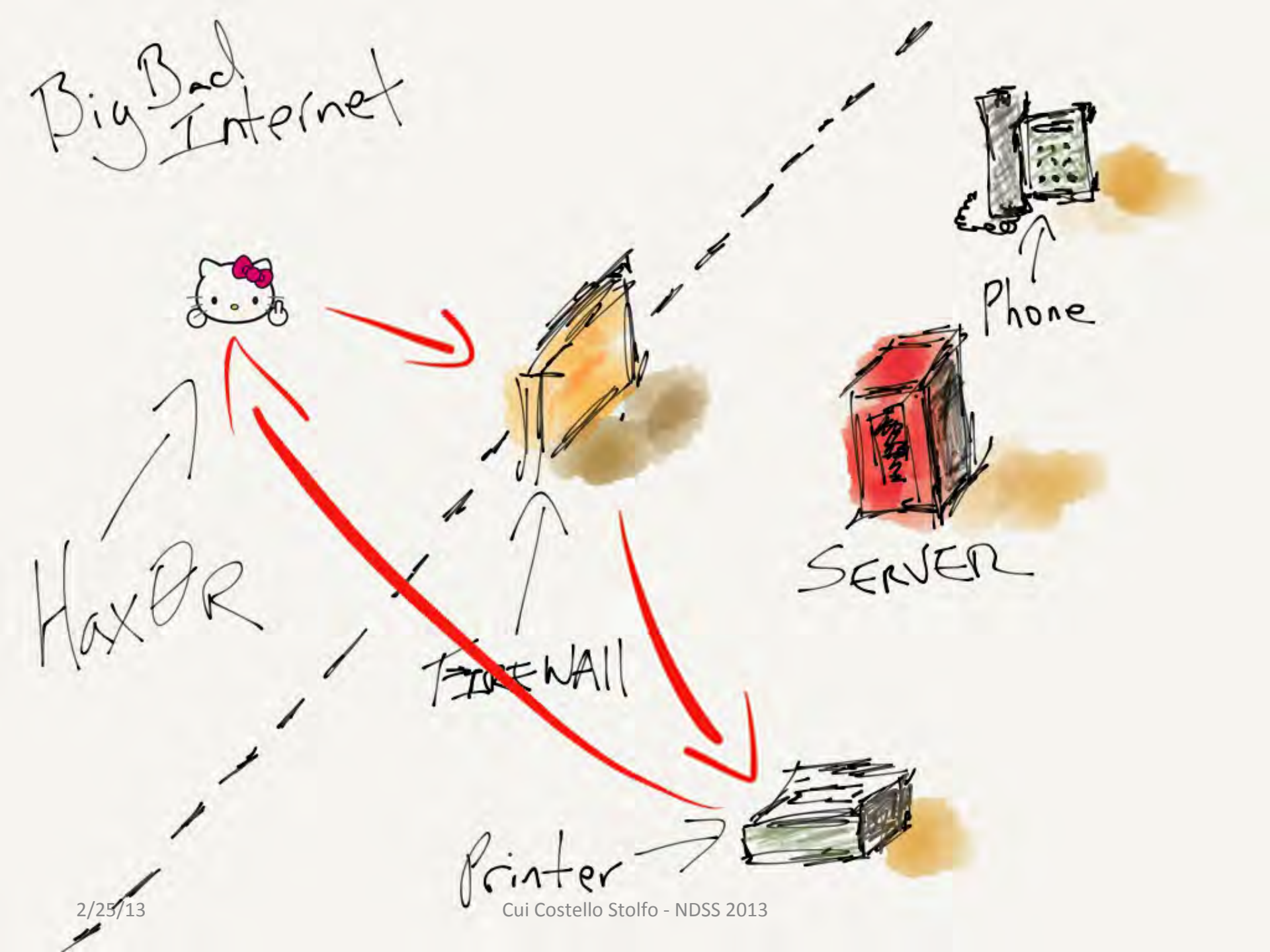

Big Bad Internet
HaxOR
FIREWALL
SERVER
Printer

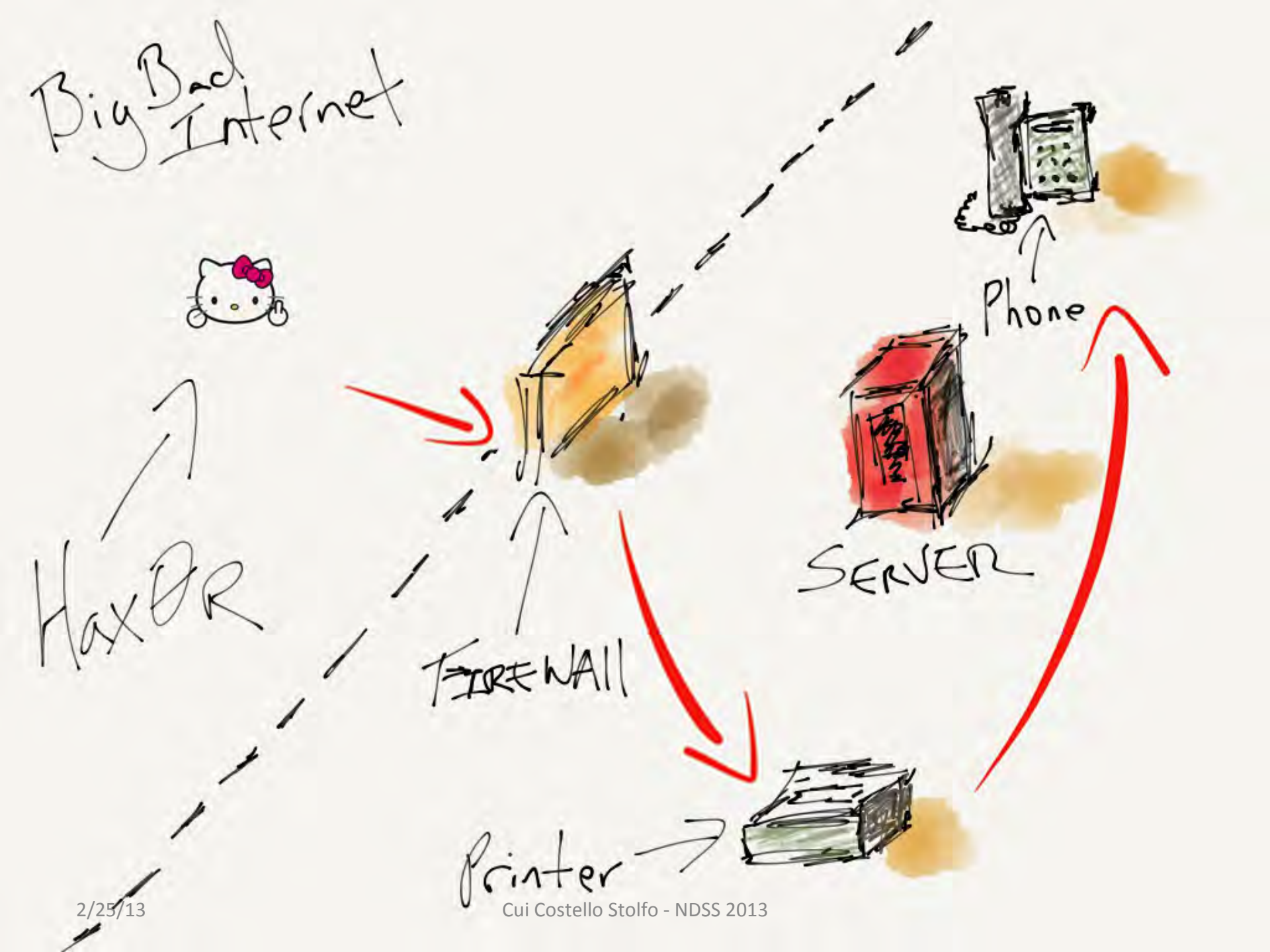

Big Bad Internet
HaxOR
FIREWALL
SERVER
Phone
Printer

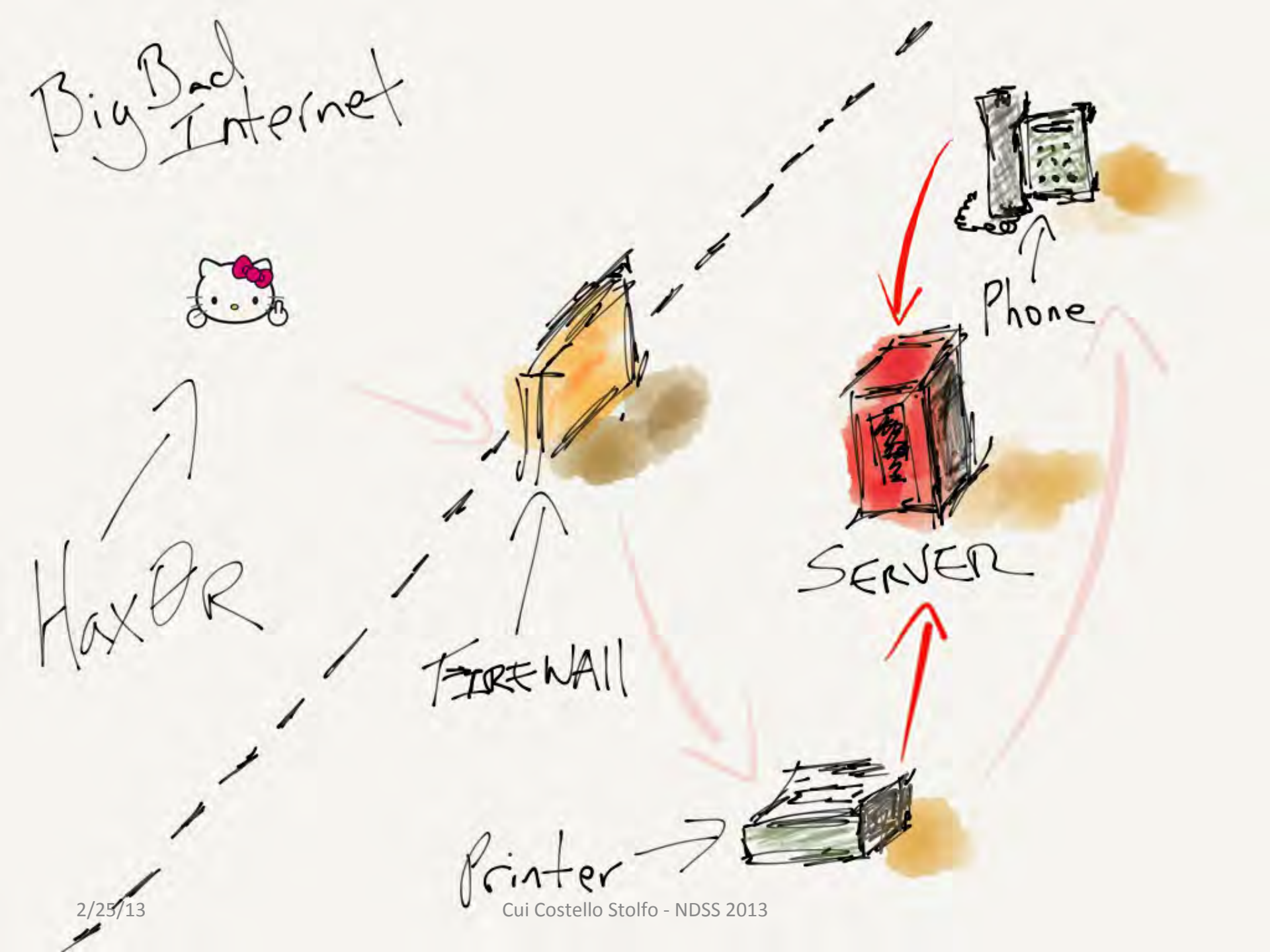

In 2KNow...

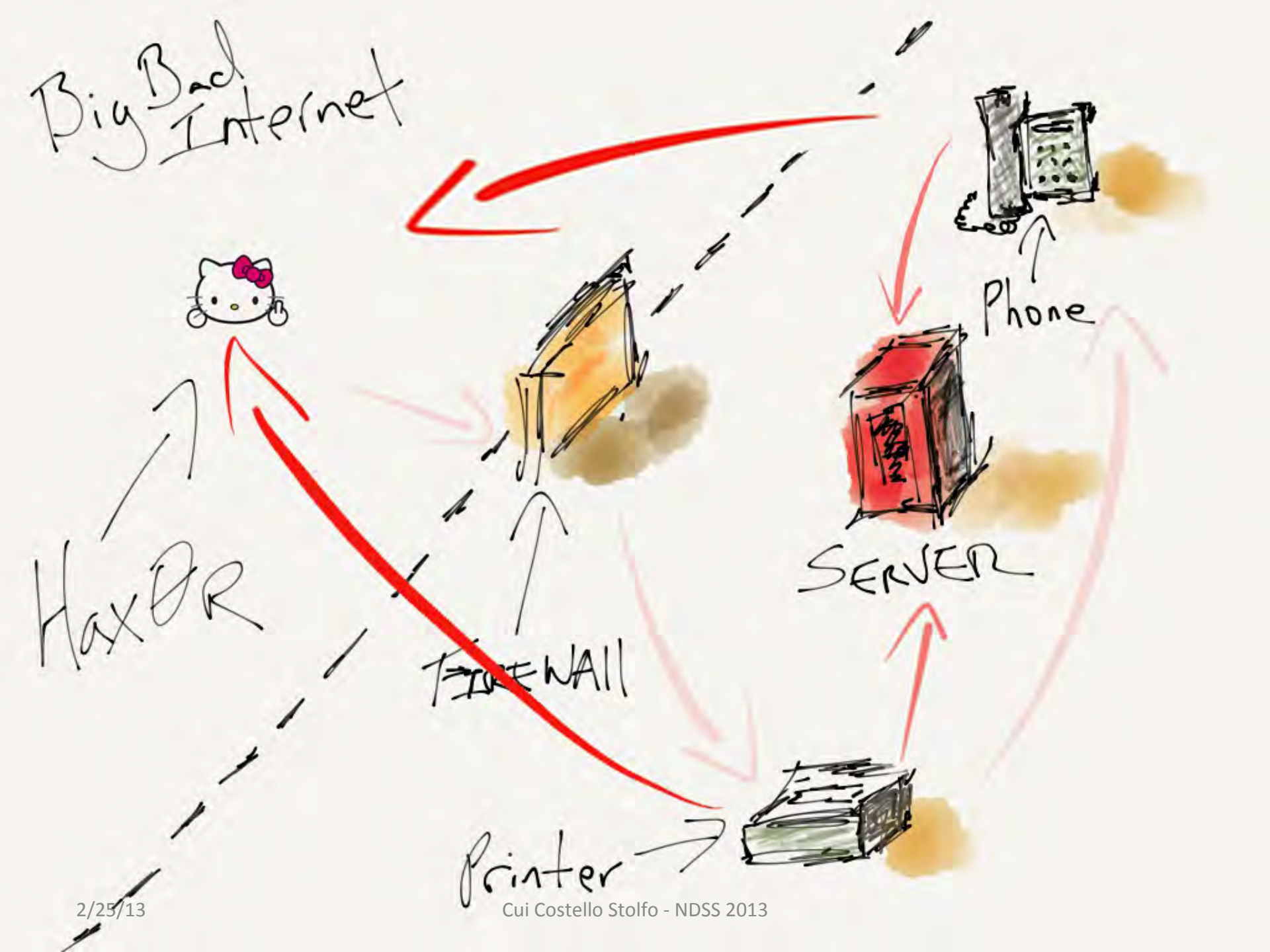

Big Bad Internet
HaxOR
FIREWALL
Phone
SERVER
Printer


Big Bad Internet
HaxOR
FIREWALL
SERVER
Phone
Printer


Big Bad Internet
Phone
HaxOR
SERVER
FIREWALL
Printer


Big Bad Internet
HaxOR
FIREWALL
SERVER
Phone
Printer


Big Bad Internet
HaxOR
FIREWALL
SERVER
Phone
Printer


Big Bad Internet
Phone
HaxOR
SERVER
FIREWALL
Printer

Let's Talk

HP Koan: How does printer update firmware?...

HP Koan: How does printer update firmware?... Print!

HP Koan: How does printer update firmware?... Print!

Remote firmware update using the LPR command

NOTE: This remote firmware update method is for use in Microsoft Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003.

Complete the following steps to update the firmware by using the LPR command.

1. Type *lpr -P -S -o l -OR- lpr -S -Pbinps* , where can be either the TCP/IP address or the hostname of the product, and where is the filename of the .RFU file from a command window.

   NOTE: The parameter (-o l) consists of a lowercase "O", not a zero, and a lowercase "L", not a numeral 1. This parameter sets the transport protocol to binary mode.

2. Press `Enter` on the keyboard. The messages described in the section "Printer messages during the firmware update" appear on the control panel.

   NOTE: The product automatically restarts the firmware to activate the update. At the end of the update process, the `Ready` message appears on the control panel.

3. Type exit at the command prompt to close the command window.

You see where this is going...

Let's play… Stare at binary blob FTW

HP RFU (Remote Firmware Update) file

```
000000  40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 4D 4F 44 45 4C 3D 48   @PJL COMMENT MODEL=H
000014  50 20 4C 61 73 65 72 4A 65 74 20 50 32 30 35 35 64 6E 0A 40   P LaserJet P2055dn¼@
000028  50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 56 45 52 53 49 4F 4E 3D   PJL COMMENT VERSION=
00003C  38 33 35 30 34 0A 40 50 4A 4C 20 43 4F 4D 4D 45 4E 54 20 44   83504¼@PJL COMMENT D
000050  41 54 45 43 4F 44 45 3D 32 30 31 30 30 33 30 38 0A 40 50 4A   ATECODE=20100308¼@PJ
000064  4C 20 55 50 47 52 41 44 45 20 53 49 5A 45 3D 37 39 32 39 39   L UPGRADE SIZE=79299
000078  30 36 0A 1B 25 2D 31 32 33 34 35 58 40 50 4A 4C 20 45 4E 54   06¼%-12345X@PJL ENT
00008C  45 52 20 4C 41 4E 47 55 41 47 45 3D 41 43 4C 0D 0A 00 AC 00   ER LANGUAGE=ACL¼
0000A0  0F 00 03 62 2D 00 00 00 00 00 79 00 00 AA 55 41 54 00 00 01   ···b-·····y··UAT···
0000B4  20 00 67 FB E9 00 E2 17 03 00 00 00 00 00 67 FD 09 00 00 20    ·g·····g½···
0000C8  E0 00 00 4D 3C 00 68 1D E9 00 00 21 86 00 00 50 91 00 68 3F   ···M<·h·····!···P·h?
0000DC  6F 00 00 20 28 00 00 4D AA 00 68 5F 97 00 00 20 BC 00 00 50   o·· (··M·h_··· ···P
0000F0  0C 00 68 80 53 00 00 20 CB 00 00 4C C4 00 68 A1 1E 00 00 20   ¼·h·S·· ···L·h····
000104  83 00 00 4D BF 00 68 C1 A1 00 00 20 23 00 00 4B 2A 00 68 E1    ···M·h··· ··#··K*·h
000118  C4 00 00 1F E1 00 00 4B D8 00 69 01 A5 00 00 20 84 00 00 4D   ····ß··K·i·¥·· ···M
00012C  5A 00 69 22 29 00 00 21 1D 00 00 4E 12 00 69 43 46 00 00 21   Z·i")··!···N··iCF··!
000140  42 00 00 50 24 00 69 64 88 00 00 24 0D 00 00 54 2D 00 69 88   B··P$·id···$♪···T-·i
000154  95 00 00 24 35 00 00 54 C1 00 69 AC CA 00 00 23 84 00 00 50    ···$5··T·i···#···P
000168  E7 00 69 D0 4E 00 00 28 24 00 00 7A 8E 00 69 F8 72 00 00 22   ·i·N··($··z·i·r··"
00017C  CD 00 00 50 D6 00 6A 1B 3F 00 00 21 3E 00 00 52 CF 00 6A 3C   ···P·j←?··!>··R·j<
000190  7D 00 00 1F F3 00 00 4B C0 00 6A 5C 70 00 00 22 11 00 00 51   }···≤··K·j\p··"···Q
```

- LPR / Raw printing has NO AUTHENTICATION mechanism

Stating the Obvious

- LPR / Raw printing has no authentication mechanism
- PJL can be embedded in postscript (and lots else)

Stating the Obvious

- LPR / Raw printing has no authentication mechanism
- PJL can be embedded in postscript (and lots else)

- Malicious RFU + Doc Format Attack Vector

  self-propagating printer malware
  embedded Advanced Persistent Asset
  Embedded spear-phishing, etc

- Reverse RFU Format
- Construct printer rootkit
- Repack malicious RFU
- Embed in document

What didn't work…

- Stare at binary blob
- Common FS headers
- Googling

What did work…

- Reversing the bootloader

What did work…

- Reversing the bootloader

- Monkey soldering
- Arduino

- Duct-tape

Reverse RFU Format

2055DN Formatter Board

Main SoC Boots from
SPI flash chip

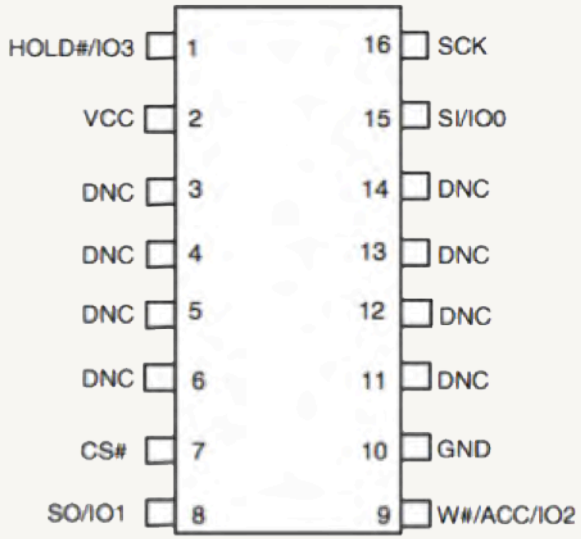
Main SoC = Mystery ARM
No datasheet

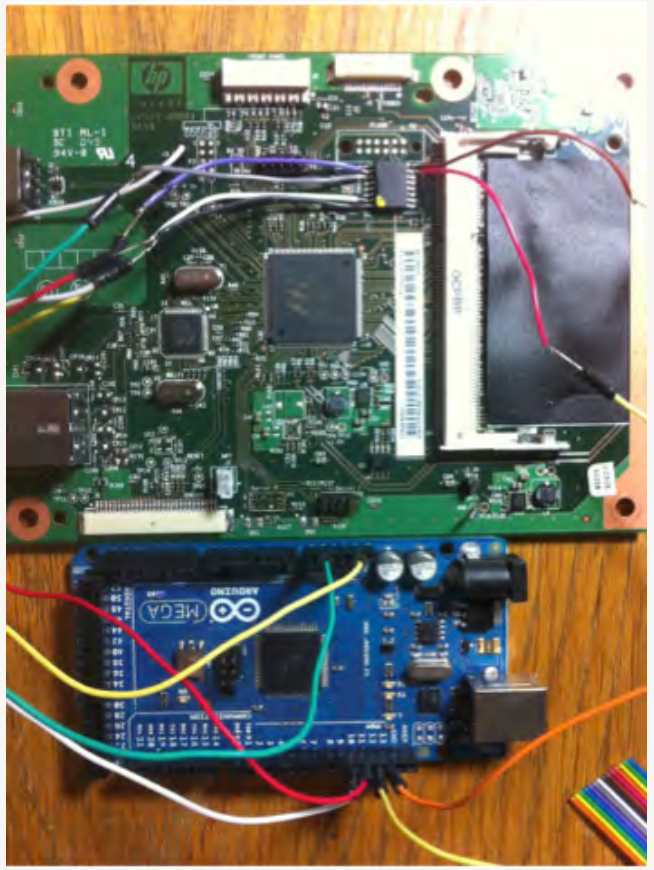
Spansion Flash
Have datasheet!

Operation	Command	One Byte Command Code	Description	Address Bytes	Mode Bit Cycle	Dummy Bytes	Data Bytes
Read	READ	**(03h)** 0000 0011	Read Data bytes	3	0	0	1 to ∞
	FAST_READ	**(0Bh)** 0000 1011	Read Data bytes at Fast Speed	3	0	1	1 to ∞
	DOR	**(3Bh)** 0011 1011	Dual Output Read	3	0	1	1 to ∞
	QOR	**(6Bh)** 0110 1011	Quad Output Read	3	0	1	1 to ∞
	DIOR	**(BBh)** 1011 1011	Dual I/O High Performance Read	3	1	0	1 to ∞
	QIOR	**(EBh)** 1110 1011	Quad I/O High Performance Read	3	1	2	1 to ∞
	RDID	**(9Fh)** 1001 1111	Read Identification	0	0	0	1 to 81
	READ_ID	**(90h)** 1001 0000	Read Manufacturer and Device Identification	3	0	0	1 to ∞
Write Control	WREN	**(06h)** 0000 0110	Write Enable	0	0	0	0
	WRDI	**(04h)** 0000 0100	Write Disable	0	0	0	0
Erase	P4E	**(20h)** 0010 0000	4 KB Parameter Sector Erase	3	0	0	0
	P8E	**(40h)** 0100 0000	8 KB (two 4 KB) Parameter Sector Erase	3	0	0	0
	SE	**(D8h)** 1101 1000	64 KB Sector Erase	3	0	0	0
	BE	**(60h)** 0110 0000 or **(C7h)** 1100 0111	Bulk Erase	0	0 0	0 0	0
Program	PP	**(02h)** 0000 0010	Page Programming	3	0	0	1 to 256
	QPP	**(32h)** 0011 0010	Quad Page Programming	3	0	0	1 to 256
Status & Configuration Register	RDSR	**(05h)** 0000 0101	Read Status Register	0	0	0	1 to ∞
	WRR	**(01h)** 0000 0001	Write (Status & Configuration) Registers	0	0	0	1 to 2
	RCR	**(35h)** 0011 0101	Read Configuration Register (CFG)	0	0	0	1 to ∞
	CLSR	**(30h)** 0011 0000	Reset the Erase and Program Fail Flag (SR5 and SR6) and restore normal operation)	0	0	0	1
Power Saving	DP	**(B9h)** 1011 1001	Deep Power-Down	0	0	0	0
	RES	**(ABh)** 1010 1011	Release from Deep Power-Down Mode	0	0	3	0
		(ABh) 1010 1011	Release from Deep Power-Down and Read Electronic Signature	0	0	0	1 to ∞
OTP	OTPP	**(42h)** 0100 0010	Programs one byte of data in OTP memory space	3	0	1	1
	OTPR	**(4Bh)** 0100 1011	Read data in the OTP memory space	3	0	0	1 to ∞

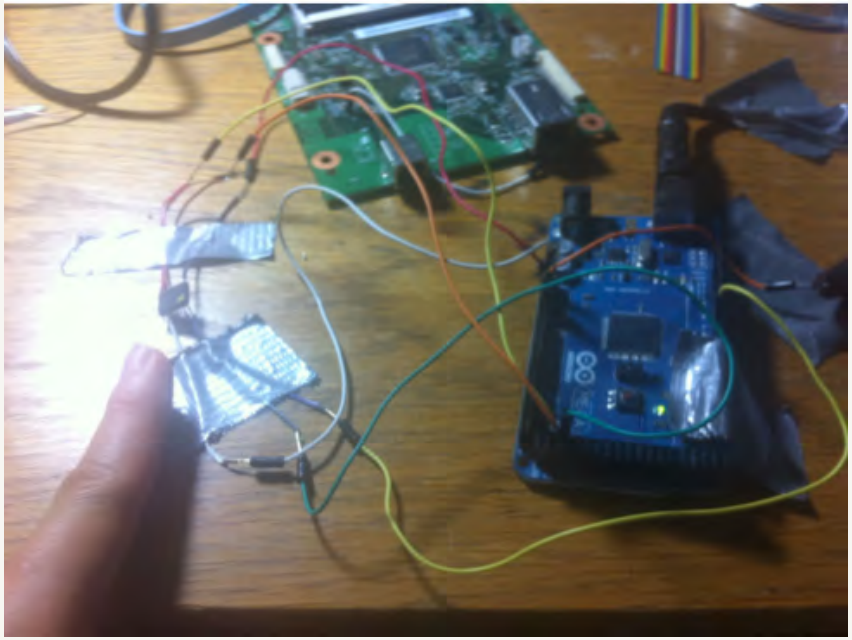
Reverse RFU Format

Figure 2.1 16-pin Plastic Small Outline Package (SO)





Reverse RFU Format



Reverse RFU Format

0000002F	C	VerifyUSBID: NO MATCH, was %s, should be: %s\r\n
0000003D	C	VerifyUSBID: NO MATCH, USBID sent: %s, USBID should be: %s\r\n
0000004E	C	VerifyFWKey: NVRAM Key: 0x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x
0000004E	C	VerifyFWKey: Sent Key: 0x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%2x%
0000003D	C	VerifyFWKey: NO MATCH at byte %d - NVRAM:0x%2x Sent:0x%2x \r
00000039	C	VerifyFWKey: Super Secret Bypass of Crypto-Key enabled\r\n
0000005B	C	VerifyPlatformID: ERROR: Invalid ID info version. Should be %d, %d,
0000002A	C	ACLBurnFlash: dataLen = %d, offset = %d\r\n
0000002C	C	ACLBurnFlash: Downloading %d bytes to %#x\r\n
0000002D	C	ACLBurnFlash: Boot bank %d, Target bank %d\r\n
00000039	C	ACLBurnFlash: FLASH sector size 0x%x (%x boot sectors)\r\n

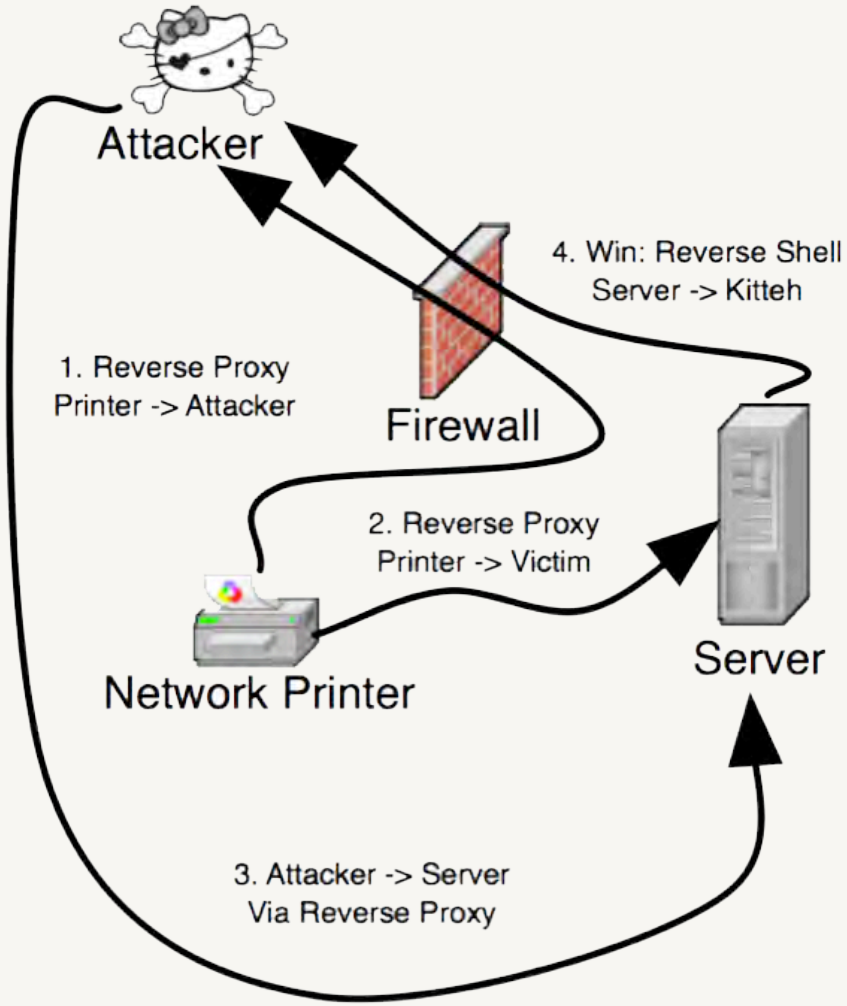
Awesomesauce!

Security Analysis

- No memory-space isolation / separation
- No "kernel"-level security
- Everything runs as supervisor mode on CPU

- Any vulnerability anywhere leads to full compromise

PoC Printer Rootkit

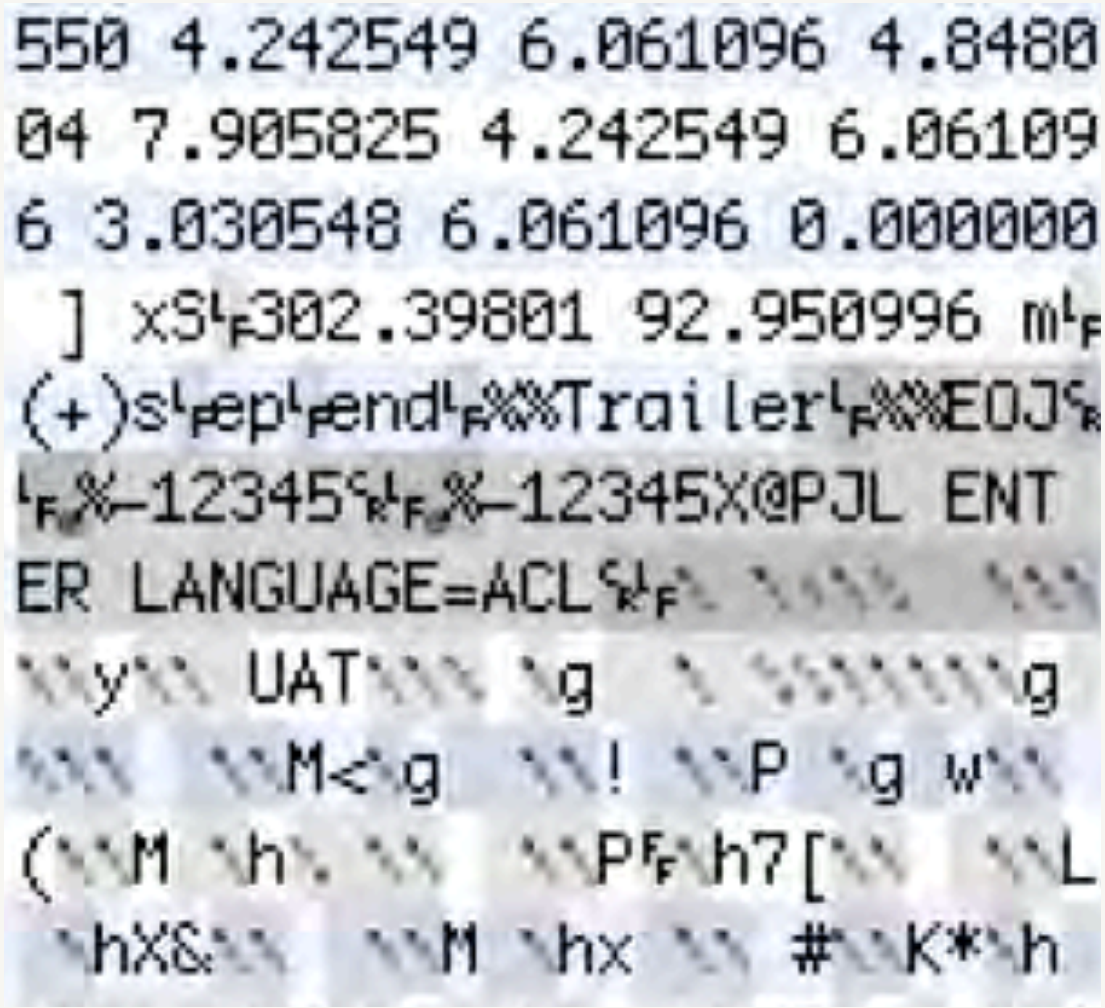


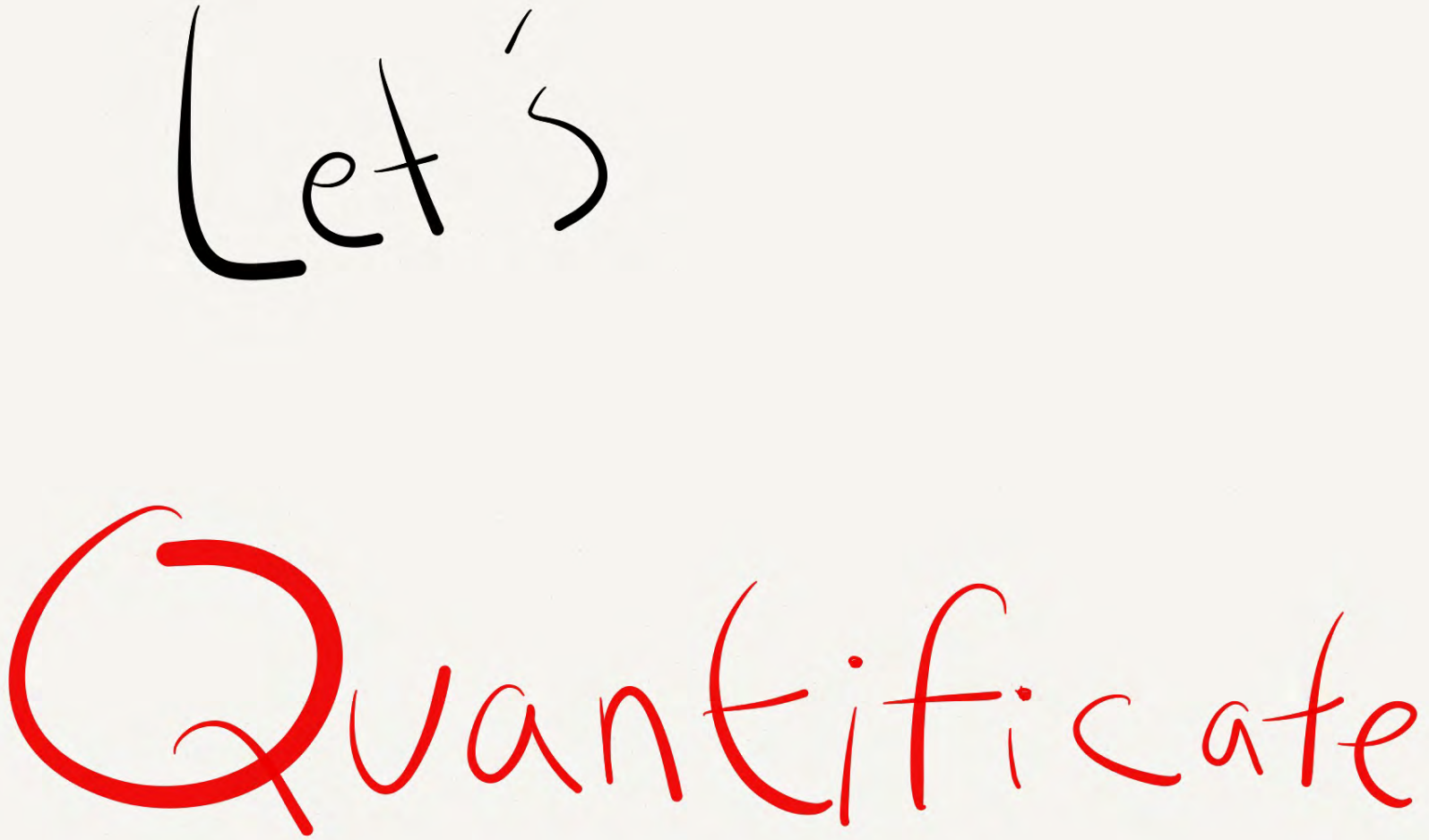
- 3KB of ARM assembly
- Print-job interceptor
- Reverse-IP Proxy

- Engine-controller hijacker

- Live Demo @ 28C3

Embed in Doc (reflexive Attack)




Let's
Quantificate

DISCLOSURE: NOVEMBER 21ST

FIRMWARE RELEASE: DECEMBER 23RD

56

PRINTER FIRMWARES HAVE BEEN UPDATED

2005 - 2011

HP LaserJet Pro 100 color MFP M175
HP LaserJet Pro CP1025 Color Printer series
HP LaserJet Pro P1102 Printer series
HP LaserJet M1120 Multifunction Printer series
HP LaserJet Pro M1136 Multifunction Printer series
HP Color LaserJet CP1210 Printer series
HP LaserJet Pro M1212nf Multifunction Printer series
HP Color LaserJet CM1312 Multifunction Printer
HP Color LaserJet CM1312nfi Multifunction Printer
HP LaserJet M1319 Multifunction Printer series
HP LaserJet Pro CM1415 Color Multifunction Printer
HP LaserJet P1500 Printer series
HP Color LaserJet CP1510 Printer series
HP LaserJet M1522 Multifunction Printer
HP LaserJet Pro CP1525 Color Printer
HP LaserJet Pro M1536 Multifunction Printer
HP LaserJet Pro P1606dn
HP Color LaserJet CP2025
HP LaserJet P2035
HP LaserJet P2055
HP Color LaserJet CM2320 Multifunction
HP LaserJet 2400 Printer series
HP LaserJet M2727 Multifunction Printer
HP Color LaserJet 2800 All-in-One Printer series
HP Color LaserJet 3000
HP LaserJet P3005
HP LaserJet Enterprise P3015
HP LaserJet M3027 Multifunction Printer
HP LaserJet M3035
HP Color LaserJet CP3505
HP Color LaserJet CP3525
HP Color LaserJet CM3530
HP Color LaserJet 3800
HP Color LaserJet CP4005
HP LaserJet P4014
HP LaserJet P4015
HP LaserJet 4240
HP LaserJet 4250
HP LaserJet 4345 Multifunction Printer
HP LaserJet M4345 Multifunction Printer
HP LaserJet 4350
HP LaserJet P4515
HP Color LaserJet Enterprise CP4525
HP Color LaserJet 4700
HP Color LaserJet 4730 Multifunction Printer
HP Color LaserJet CM4730 Multifunction
HP LaserJet M5025 Multifunction Printer
HP LaserJet M5035 Multifunction Printer
HP LaserJet 5200L
HP LaserJet 5200N
HP Color LaserJet Professional CP5225
HP Color LaserJet 5550
HP Color LaserJet CP6015
HP Color LaserJet CM6030
HP Color LaserJet CM6040
HP CM8060 Color Multifunction Printer
HP LaserJet 9040
HP LaserJet 9040 Multifunction Printer
HP LaserJet M9040 Multifunction Printer
HP LaserJet 9050
HP LaserJet 9050 Multifunction Printer
HP LaserJet M9050 Multifunction Printer
HP 9200c Digital Sender
HP 9250c Digital Sender
HP Color LaserJet 9500
HP Color LaserJet 9500 Multifunction Printer

CVE: CVE-2011-4161

SSRT: 100692 rev.6

Potentially vulnerable printers	90,847
Printers with identifiable firmware datecode	74,770
Number of patched printers	808
Overall patch rate	1.08%

TABLE I
OBSERVED POPULATION OF PRINTERS VULNERABLE TO THE HP-RFU ATTACK ON IPV4.

MONTHS AFTER PATCH RELEASE

HOW MANY VULNERABLE PRINTERS ARE THERE IN THE WORLD?

Potentially vulnerable printers	90,847
Printers with identifiable firmware datecode	74,770
Number of patched printers	808
Overall patch rate	1.08%

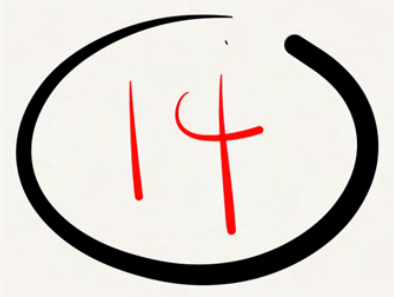
TABLE I
OBSERVED POPULATION OF PRINTERS VULNERABLE TO THE HP-RFU ATTACK ON IPV4.

MONTHS AFTER PATCH RELEASE

HOW MANY VULNERABLE PRINTERS ARE THERE IN THE WORLD?

Potentially vulnerable printers	
Printers with identifiable firmware datecode	
Number of patched printers	
Overall patch rate	

TABLE I
OBSERVED POPULATION OF PRINTERS VULNERABLE TO THE HP-RFU ATTACK ON IPV4.



MONTHS AFTER PATCH RELEASE

HOW MANY VULNERABLE PRINTERS ARE THERE IN THE WORLD?

Potentially vulnerable printers	
Printers with identifiable firmware datecode	76,288
Number of patched printers	5,659
Overall patch rate	7.42%

TABLE I

OBSERVED POPULATION OF PRINTERS VULNERABLE TO THE HP-RFU ATTACK ON IPV4.

MONTHS AFTER PATCH RELEASE

HOW MANY VULNERABLE PRINTERS ARE THERE IN THE WORLD?

Interesting Findings

- EDU HAS THE MOST VULNERABLE PRINTERS

	Count	Avg Age (years)	Oldest Firmware
Education	48,626	4.13	1993-08-20
ISP	4,650	3.70	1994-10-12
Enterprise	2,842	4.02	1992-12-16
Military	201	4.63	1999-10-30
Government	126	4.33	1996-12-20

TABLE III
ORGANIZATIONAL DISTRIBUTION OF VULNERABLE PRINTERS.

Interesting Findings

- EDU has the most vulnerable printers
- Average printer is ~4.5 years old

	Count	Avg Age (years)	Oldest Firmware
N. America	47,840	4.46	1992-12-16
Europe	14,196	4.16	1993-08-20
Asia	10,353	3.77	1998-09-02
Oceania	1,081	4.79	1998-09-02
S. America	673	3.43	1999-01-27
Africa	60	4.56	2001-04-26

Interesting Findings

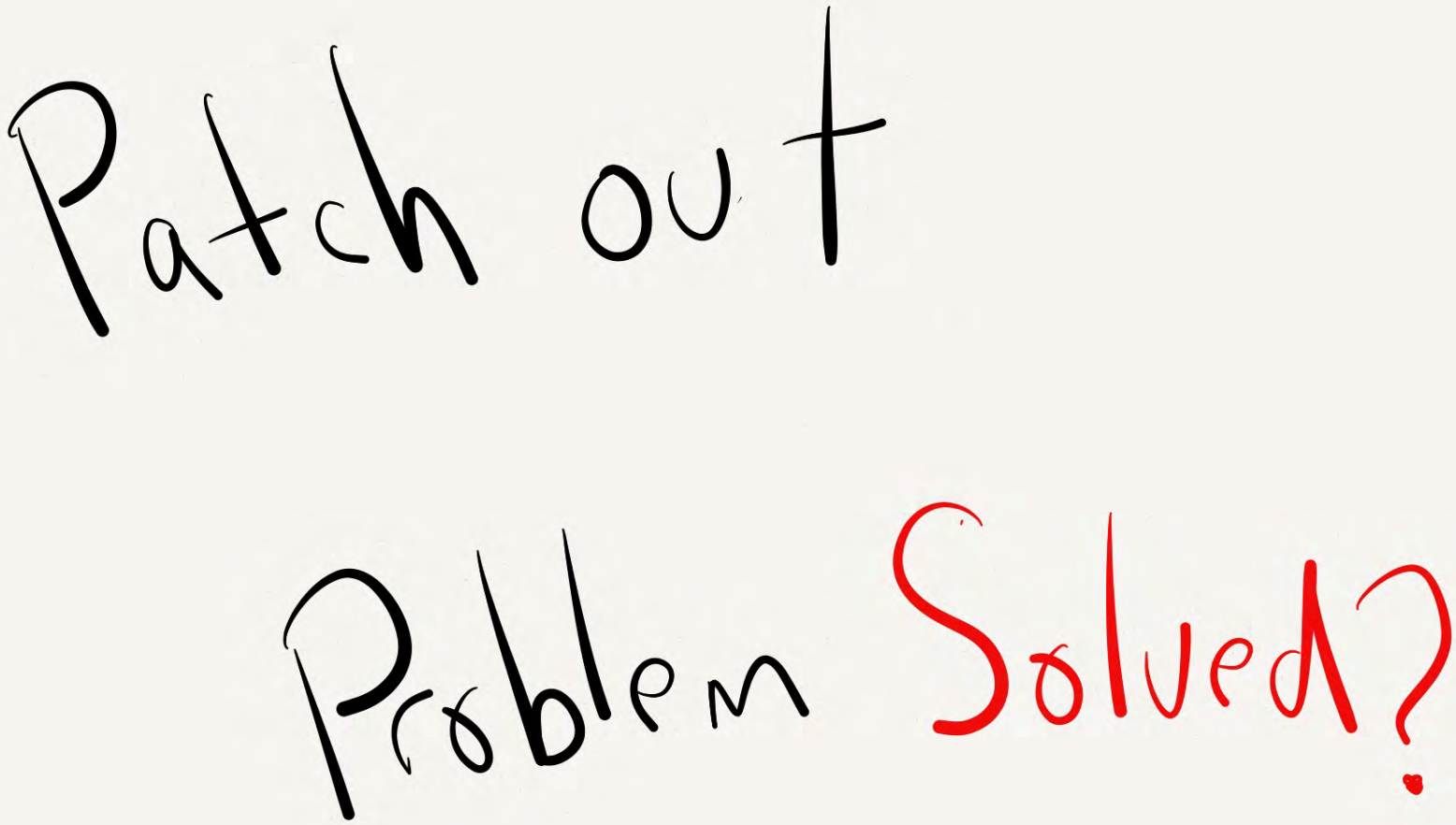
- EDU has the most vulnerable printers
- Average printer is ~4.5 years old

- Found 201 vulnerable printers in DOD (All removed)

Interesting Findings

- EDU has the most vulnerable printers
- Average printer is ~4.5 years old

- Found 201 vulnerable printers in DOD (All removed)
- Found 6 vulnerable printers in HP (3 still there)


Patch out
Problem Solved?

Vulnerable Third-Party Libraries

zlib: *CA-2002-07, CERT-{68062, 238678}* Discovered in 2002, zlib ver. 1.1.3 and earlier have a double free bug that allows arbitrary code execution [20]. In 2005 the vendor was notified of a buffer overflow in zlib ver. 1.2.1 and 1.2.2 [21]. The vendor was notified of a DOS condition in zlib ver. 1.2.0.x and 1.2.x in 2004 [22].

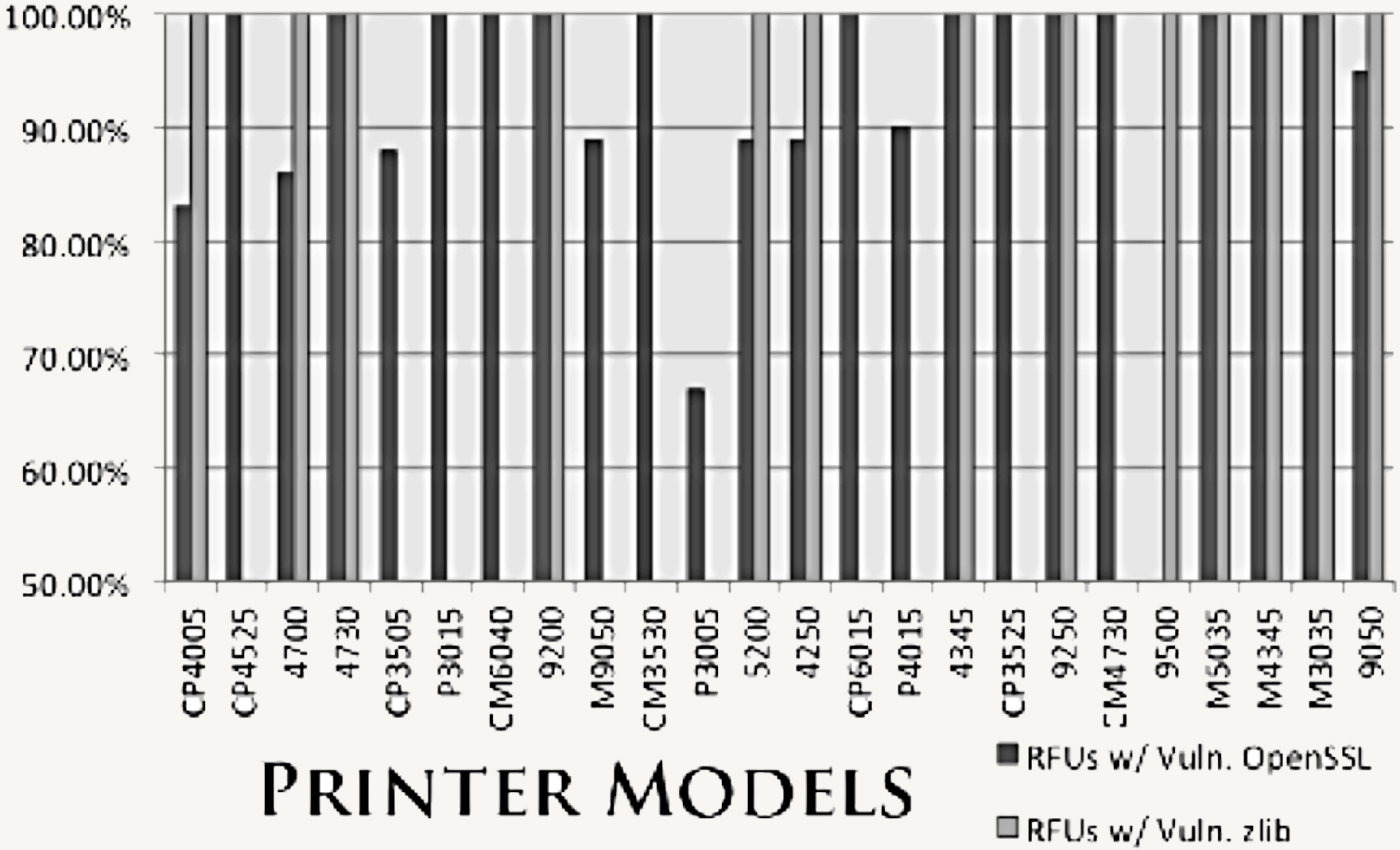
OpenSSL: *CVE-{2009-3245, 2006-3738, 2006-4339}* There are over 100 known vulnerabilities in various versions of OpenSSL. We scanned for the above three critical vulnerabilities in our firmware update dataset because they involve features that are likely to be reachable via network attack. The first two vulnerabilities can lead to arbitrary code execution. The last vulnerability can bypass x.509 certificate verification.

Printer models analyzed	63
RFU images analyzed	373
All RFUs w/ at least 1 vulnerability	300
Latest RFUs w/ at least 1 vulnerability	41 (65.1%)
Most common zlib version	1.1.4
Most common OpenSSL version	0.9.7b

TABLE VI

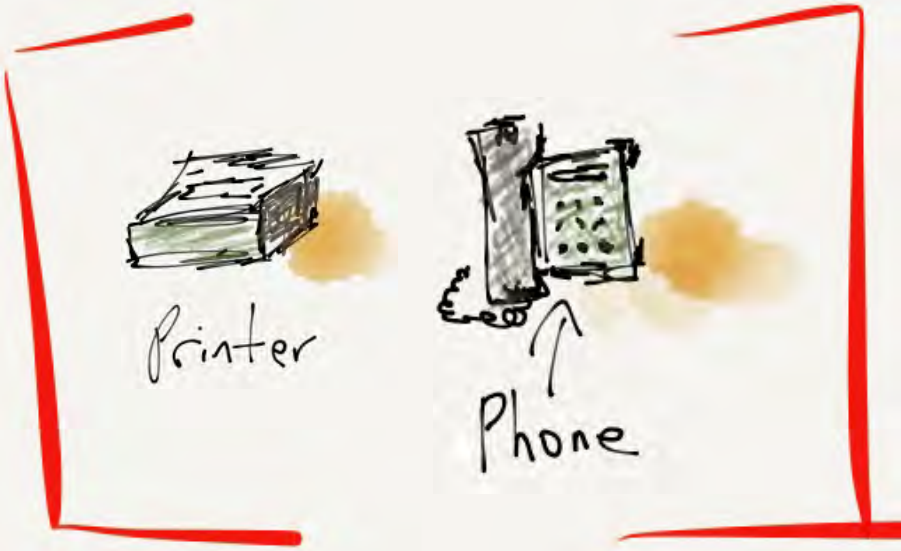
THIRD-PARTY LIBRARY VULNERABILITY ANALYSIS OBSERVATIONS.

Third-Party Library Vulnerabilities Found In Printer Firmware Updates



Take Aways

Hack A



HACK A

OWN A

Anti-Virus
IDS
Patch-Tuesday


Signed Code
≠
Secure Code


Let's Talk
DEFENSE

Meet Symbiote

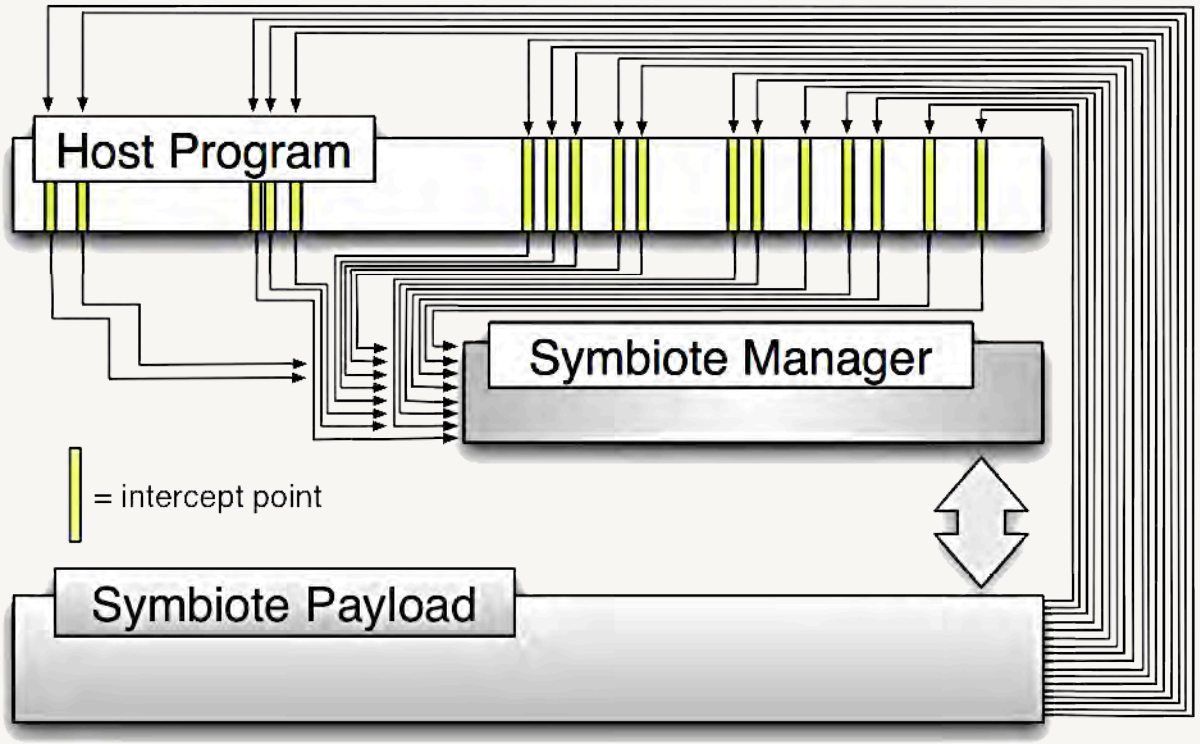
RAID 2011
Defending Legacy Embedded Systems With Software Symbiotes

ACSAC 2011
From Prey To Hunter: Transforming Legacy Embedded Devices Into Exploitation Sensor Grids

USENIX/WOOT 2011
Killing the Myth of Cisco IOS Diversity

NDSS 2013
When Firmware Modifications Attack: A Case Study of Embedded Exploitation

Symbiote Structure



Drop in a Defensive Symbiote Payload

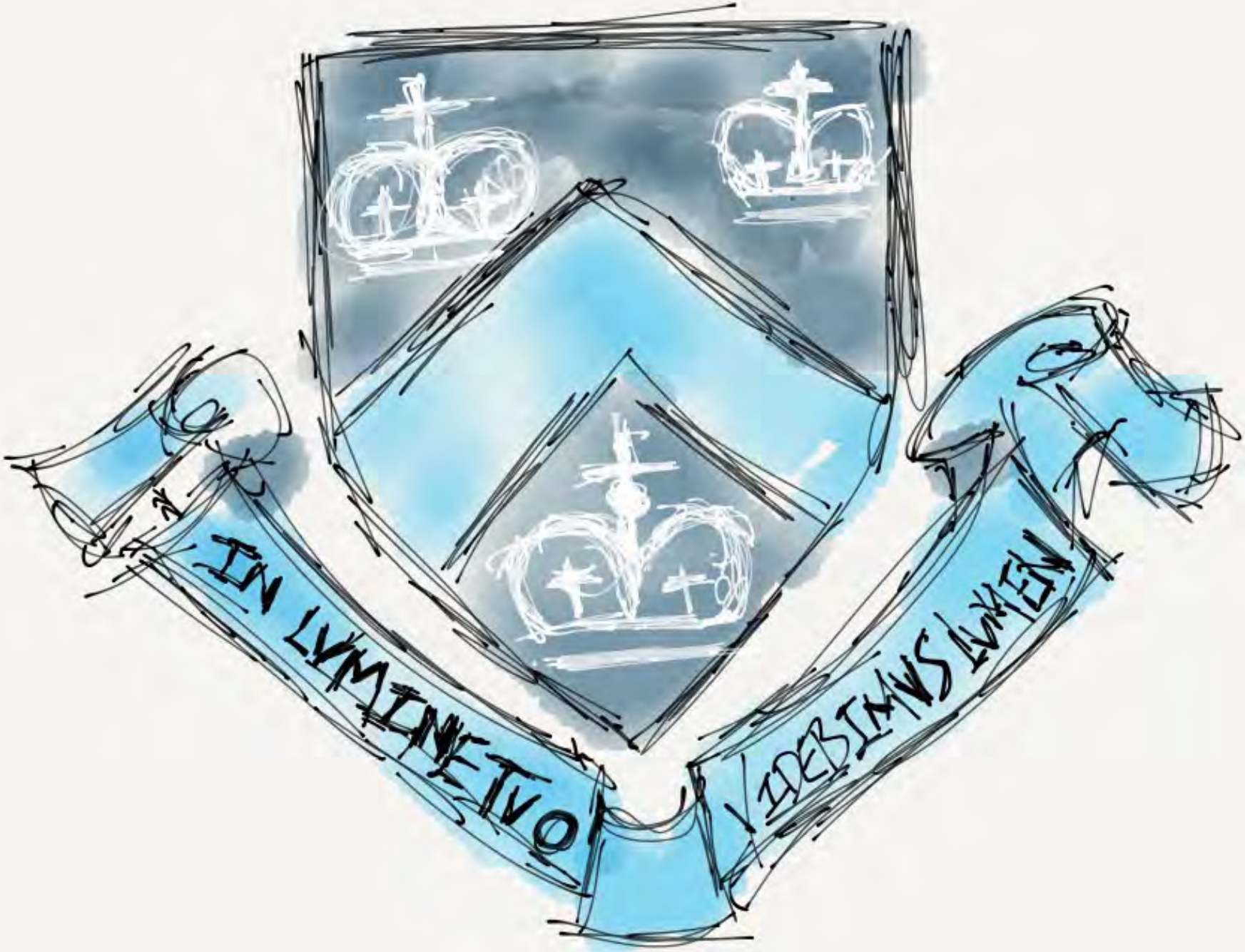
Much Thanks!

ANUP KOTALWAR
JATIN KATARIA
YUAN KANG

Much Thanks!

ANUP KOTALWAR
JATIN KATARIA
YUAN KANG

ang@cs.columbia.edu


IN LVMINE TVO
VIDEBIMVS LVMEN