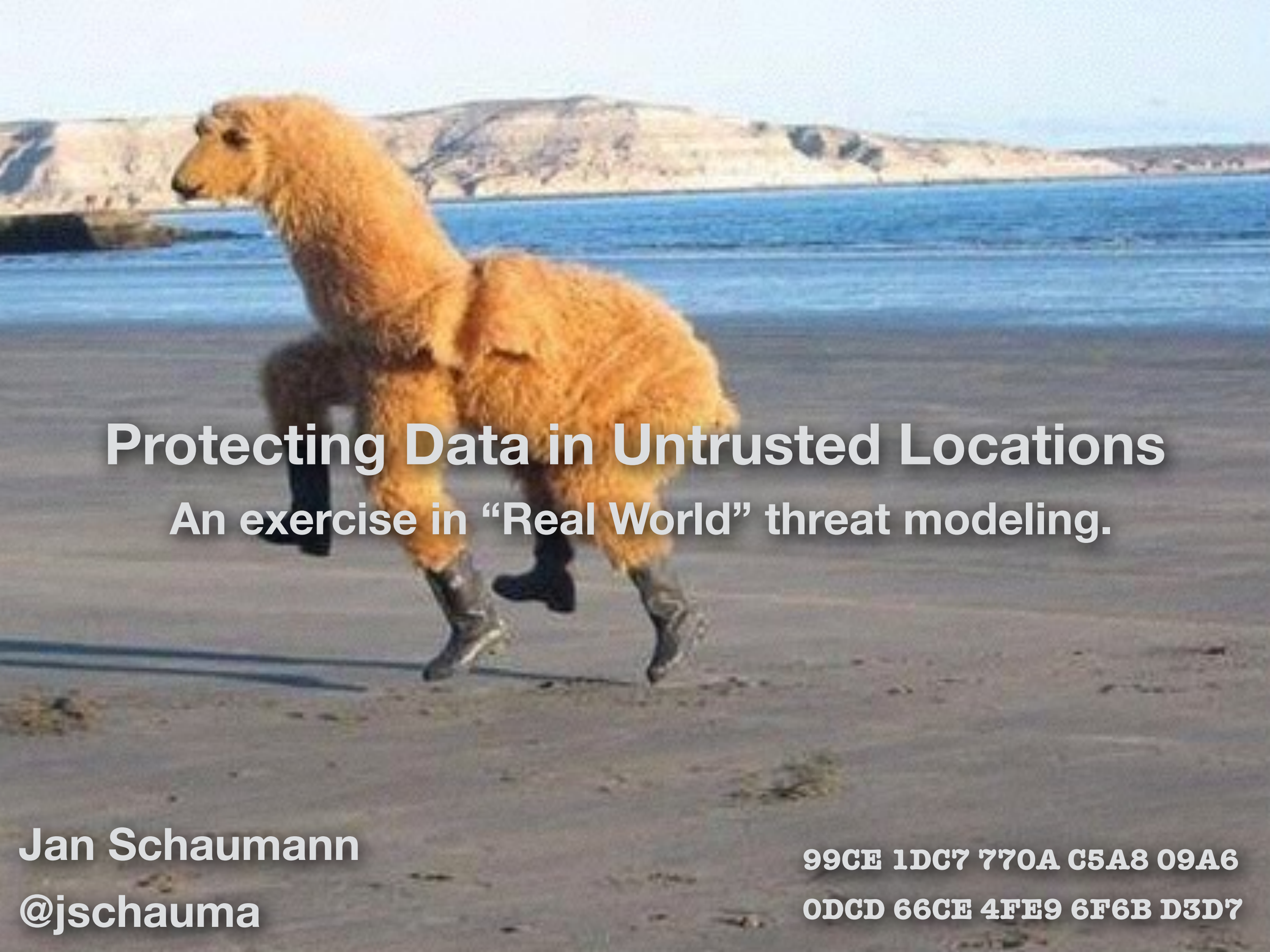


# Protecting Data in Untrusted Locations

## An exercise in “Real World” threat modeling.


Jan Schaumann

@jschauma

99CE 1DC7 770A C5A8 09A6

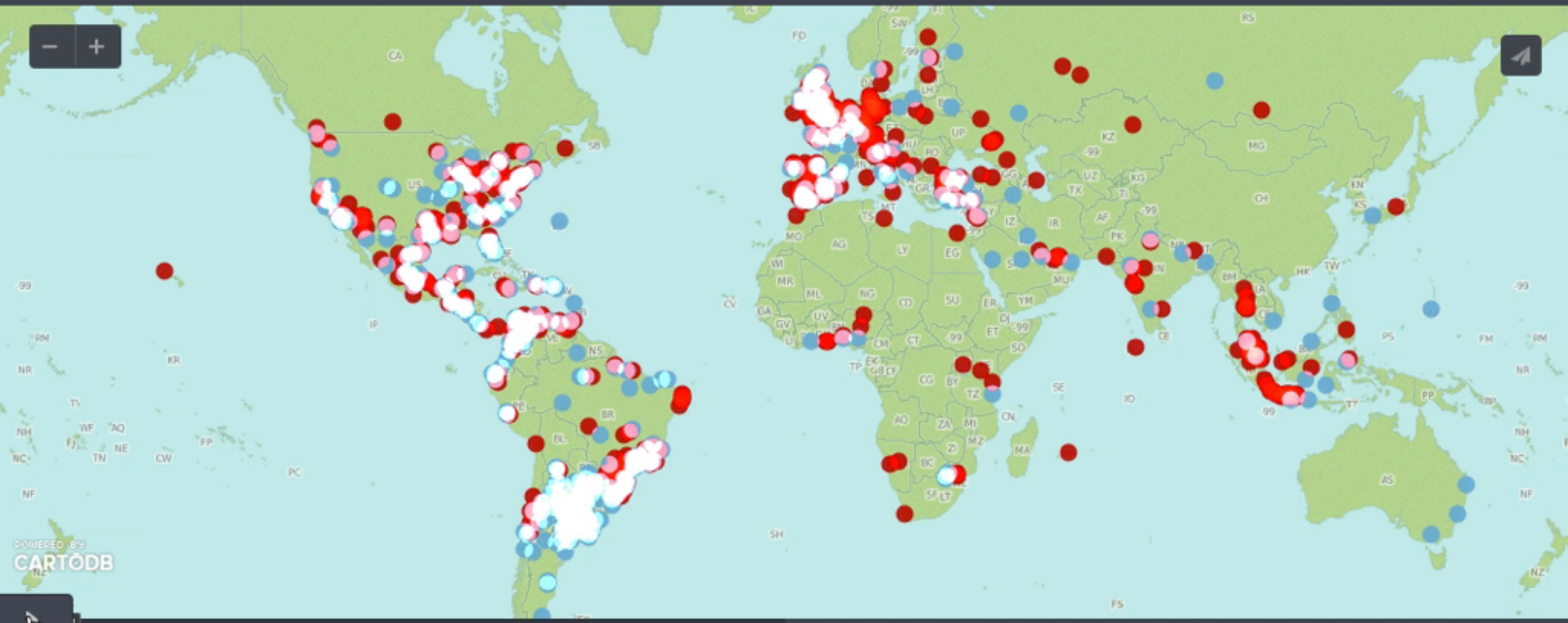
0DCD 66CE 4FE9 6F6B D3D7

I HAVE NO IDEA
WHAT I'M DOING

Me. Errday.

**WORLD CUP FINAL: #GERvARG - How Germany v Argentina played out on Twitter**

Geotagged Tweets mentioning key terms around the World Cup game, July 12, 2014, Brazil time




15:59

Germany 0 0 Argentina

cartodb.com/v/worldcup/match/?TC=x&vis=30acae6a-0a51-11e4-8918-0e73339ffa50&h=t&t=Germany,B40903|Argentina,5CA2D1&m=7/13/2014 16:00:00 GMT,7/12/2014 18:35:00GMT&g=147|#/play

Obligatory James Mickens "This World of Ours" reference.

# Threat Model

| | | | |
|---|---|---|---|
| **Threat** | Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club | Organized criminals breaking into your email account and sending spam using your identity | The Mossad doing Mossad things with your email account |
| **Solution** | Strong passwords | Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow) | ◆ Magical amulets?<br>◆ Fake your own death, move into a submarine?<br>◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON |

https://t.co/Ej94YI4Ovr

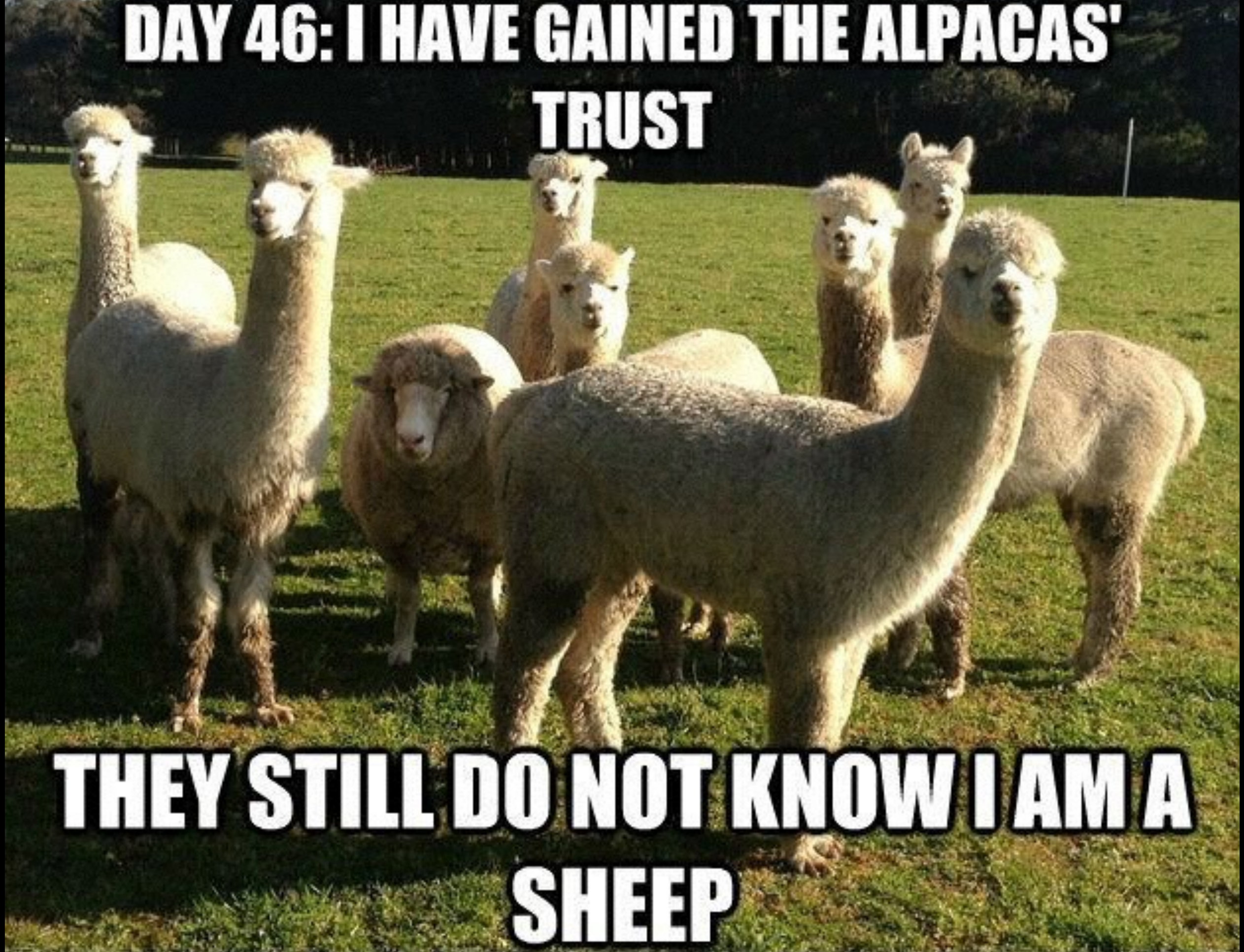
Obligatory James Mickens "This World of Ours" reference.

# Threat Model

| | | | |
|---|---|---|---|
| **Threat** | Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club | Organized criminals breaking into your email account and sending spam using your identity | The Mossad doing Mossad things with your email account |
| **Solution** | Strong passwords | Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow) | ◆ Magical amulets?<br>◆ Fake your own death, move into a submarine?<br>◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON |

https://t.co/Ej94YI4Ovr

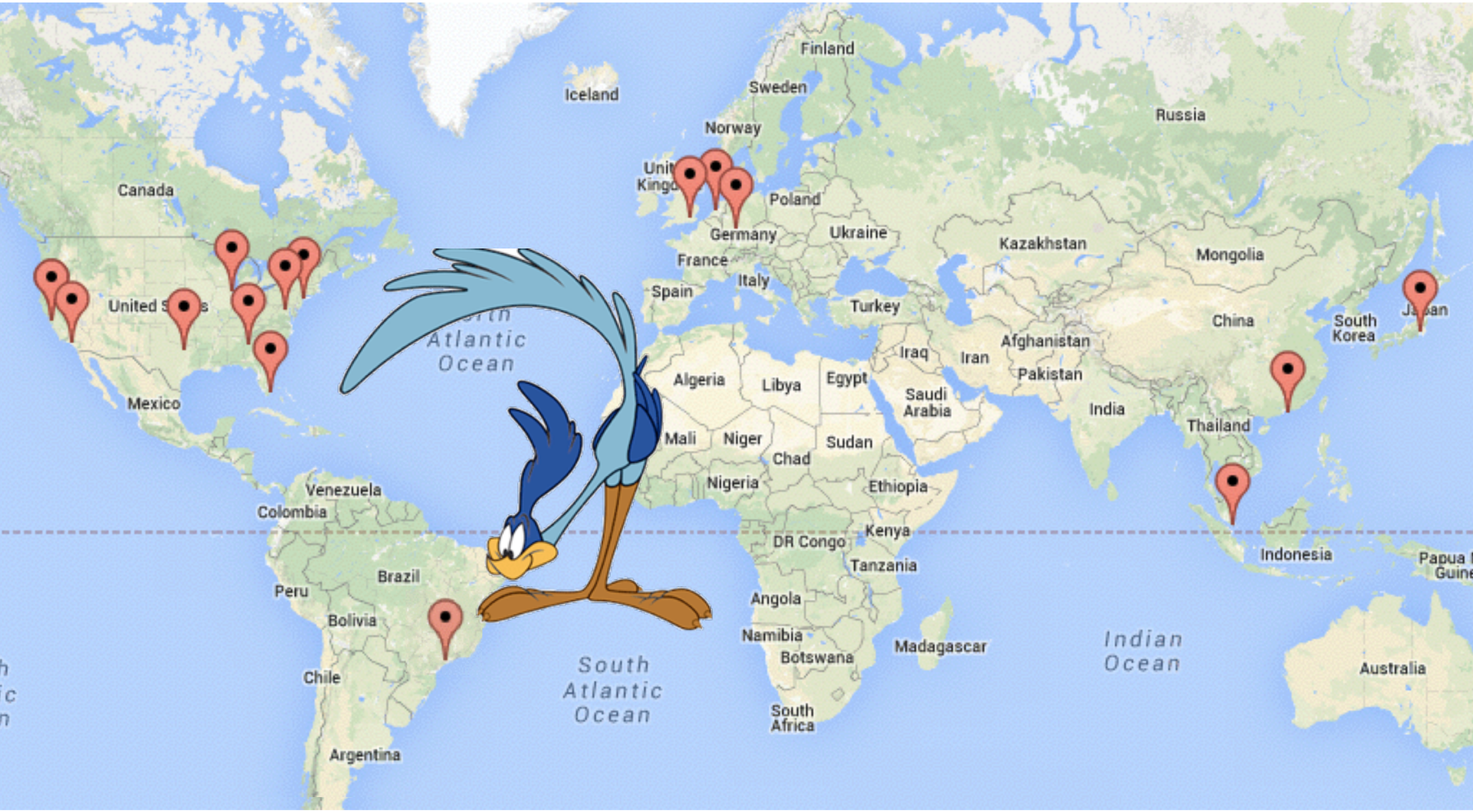
DAY 46: I HAVE GAINED THE ALPACAS' TRUST



THEY STILL DO NOT KNOW I AM A SHEEP


Tweeters
gonna tweet


https://t.co/ykdsHGV84r




https://t.co/ykdsHGV84r


https://t.co/ykdsHGV84r

# Threat Model

Threat Actors:

- *hackeris vulgaris*
- organized crime (fsvo “organized”)
- local governments or intelligence services
- foreign governments or intelligence services

# Threat Model

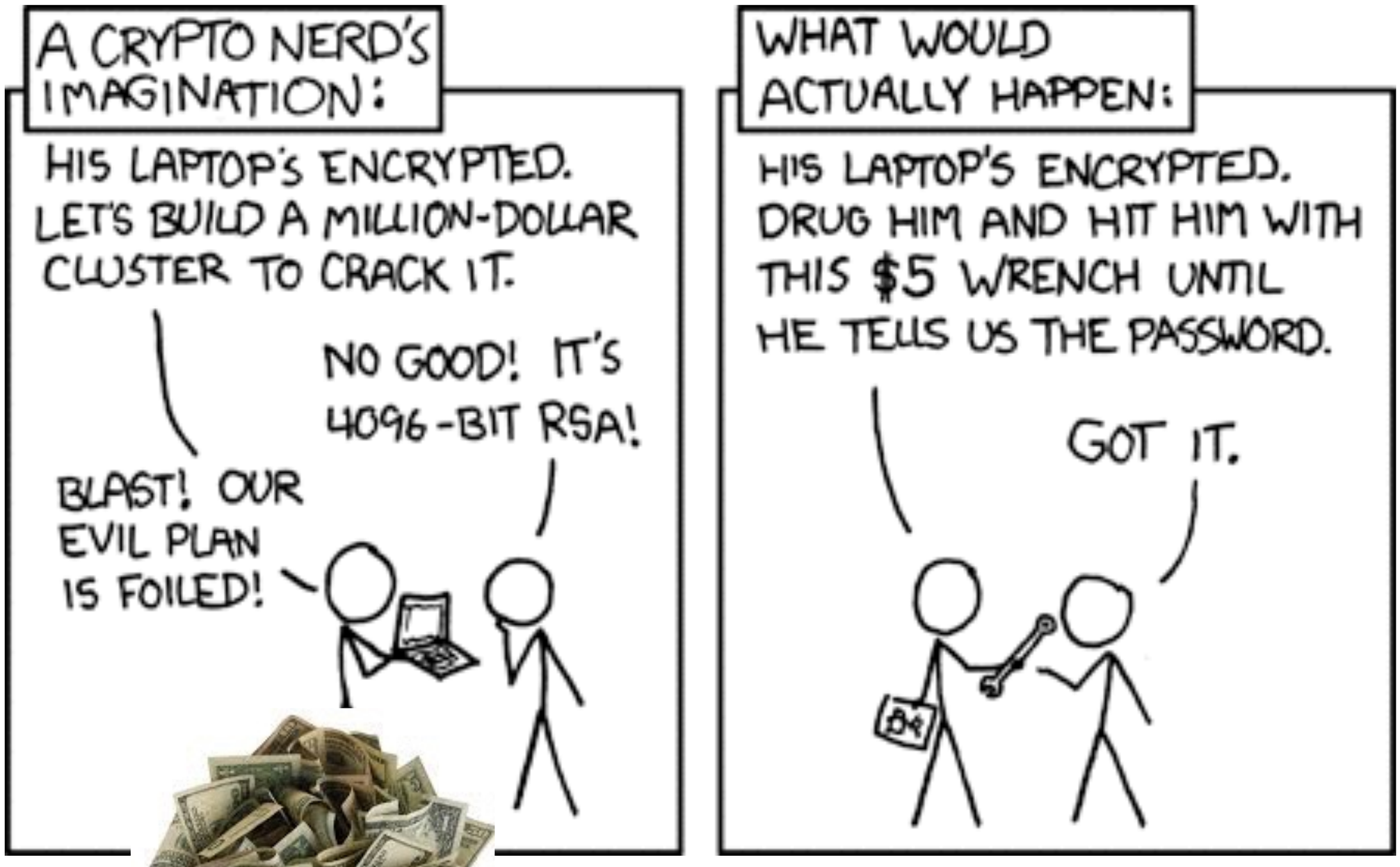
Assets:

- ~~Physical Equipment~~
- ~~Local Service Access Point~~
- Access/Entry point to Infrastructure
- TLS keys

# Access/Entry point to Infrastructure

- physically protected systems
- no “secrets” permanently stored on systems
- traffic severely restricted
- all traffic must be mutually authenticated

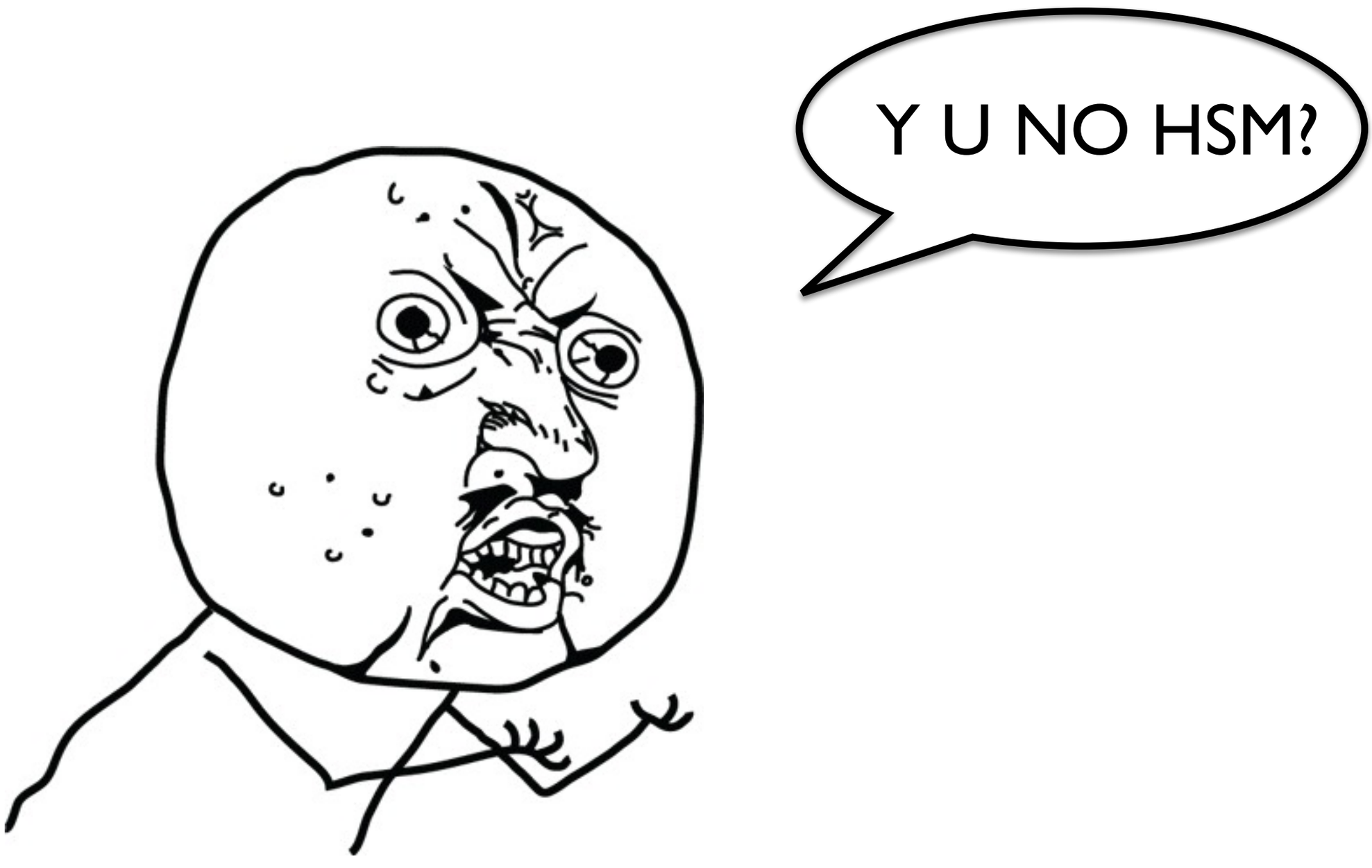
Obligatory XKCD comic.

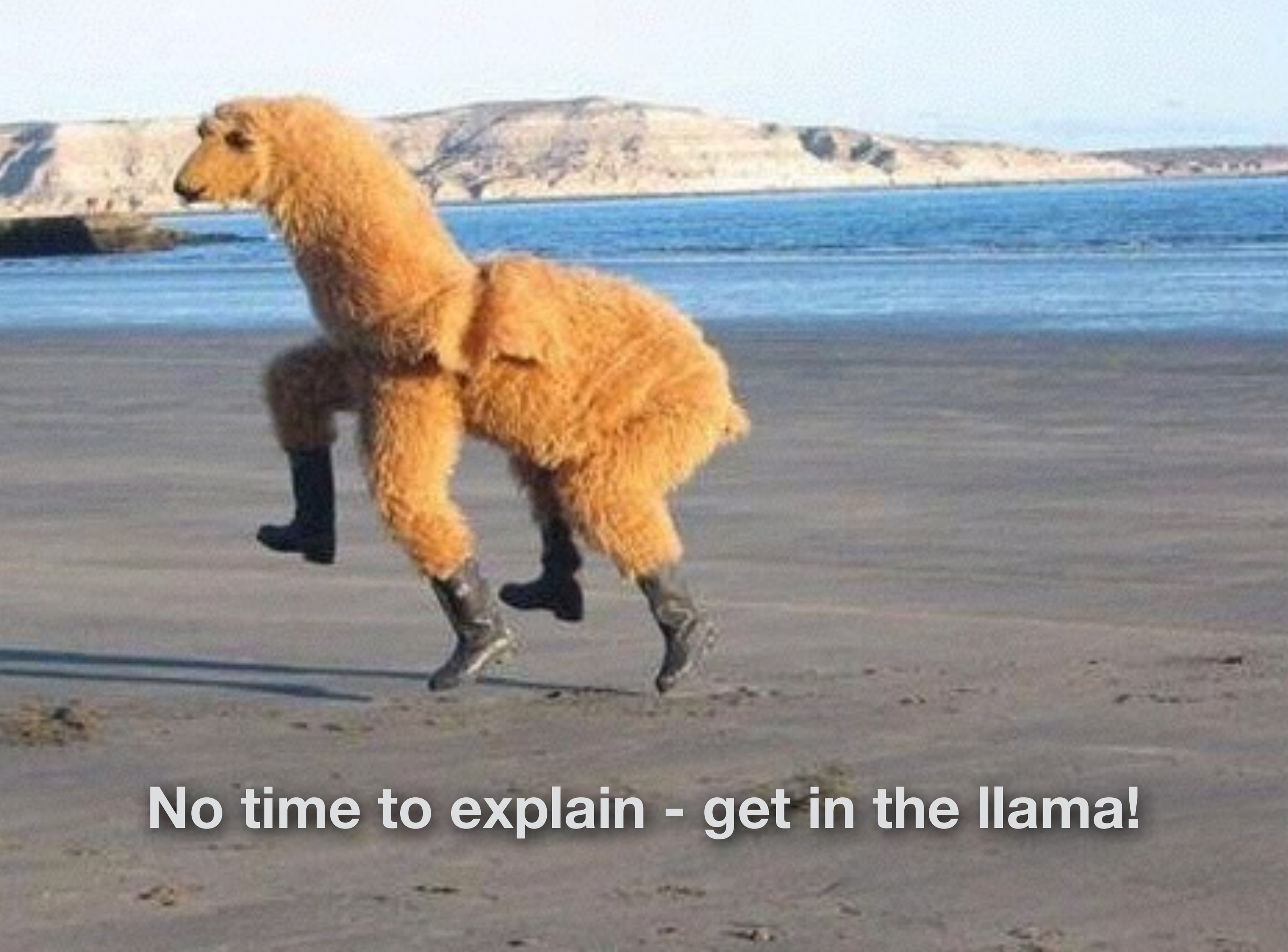



This also works.

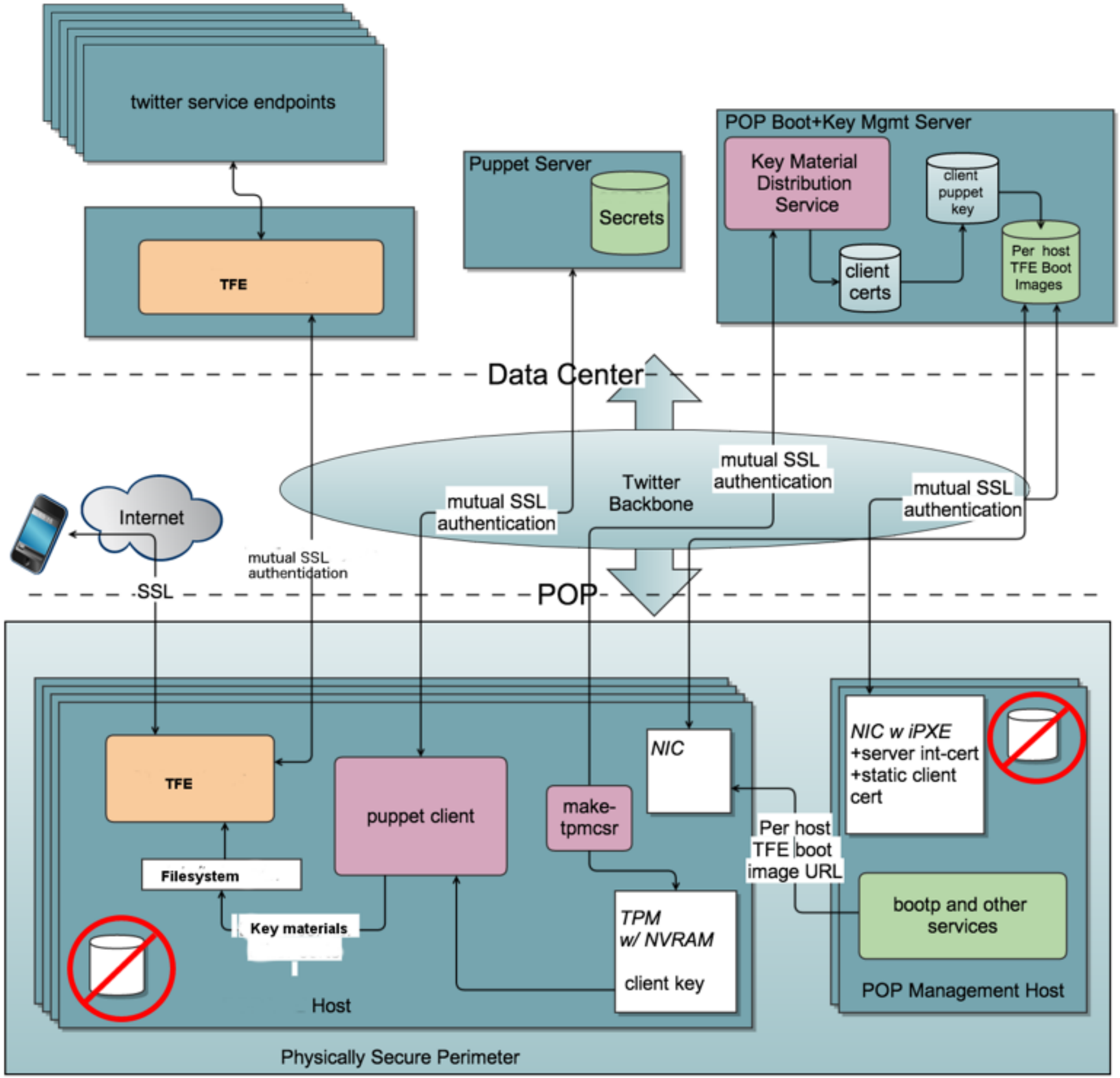
# TLS keys

# TLS keys




No time to explain - get in the llama!

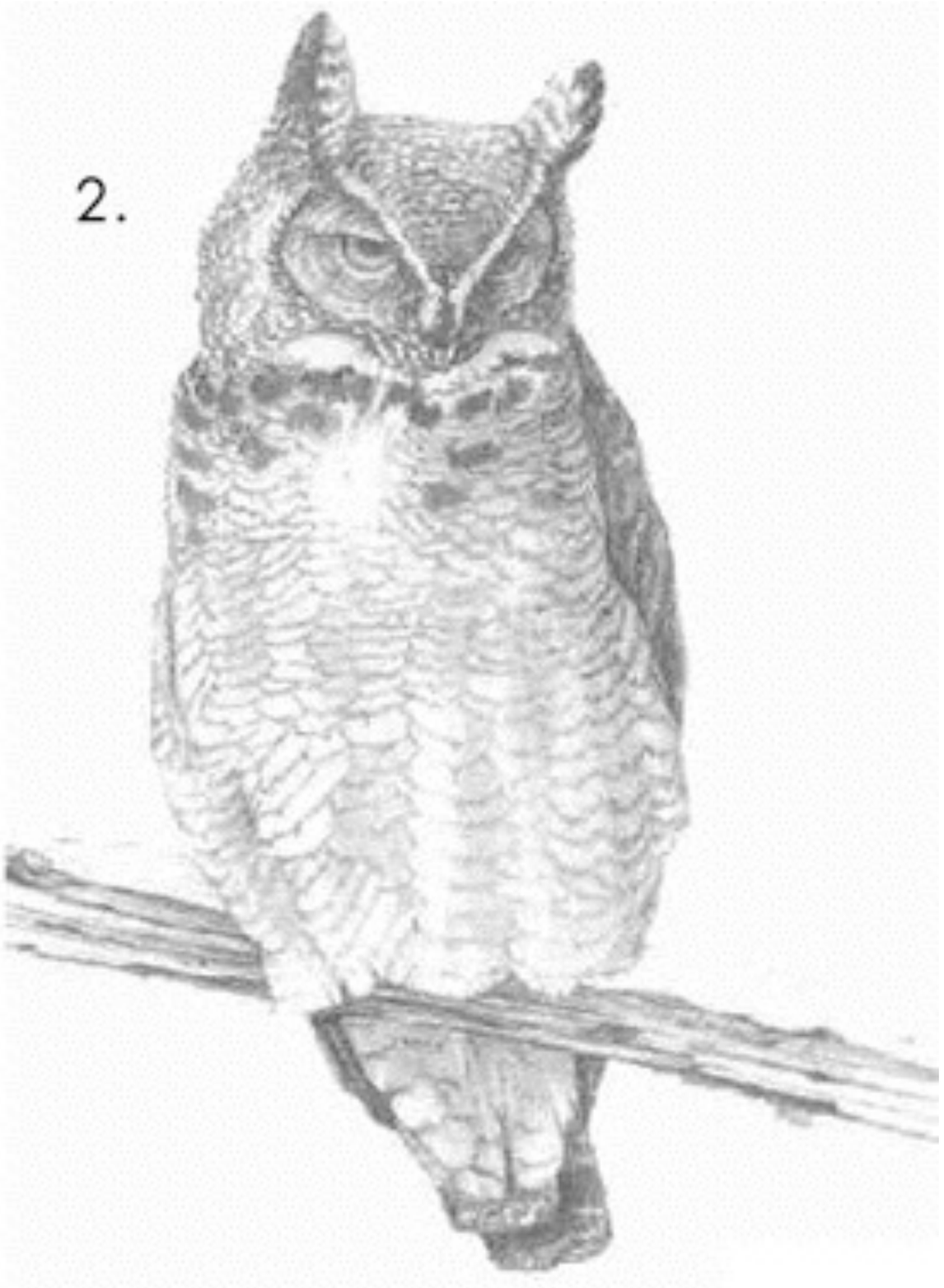

Infineon
TPM1.2
SLB 9635 TT 1.2


twitter service endpoints
TFE
Puppet Server
Secrets
POP Boot+Key Mgmt Server
Key Material Distribution Service
client puppet key
client certs
Per host TFE Boot Images
Data Center
Internet
mutual SSL authentication
Twitter Backbone
mutual SSL authentication
mutual SSL authentication
mutual SSL authentication
SSL
POP
TFE
puppet client
make-tpmcsr
NIC
NIC w iPXE
+server int-cert
+static client cert
Per host TFE boot image URL
Filesystem
Key materials
TPM w/ NVRAM
client key
bootp and other services
Host
POP Management Host
Physically Secure Perimeter

How to draw an owl

1.

2.



1. Draw some circles

2. Draw the rest of the fucking owl

# Booting

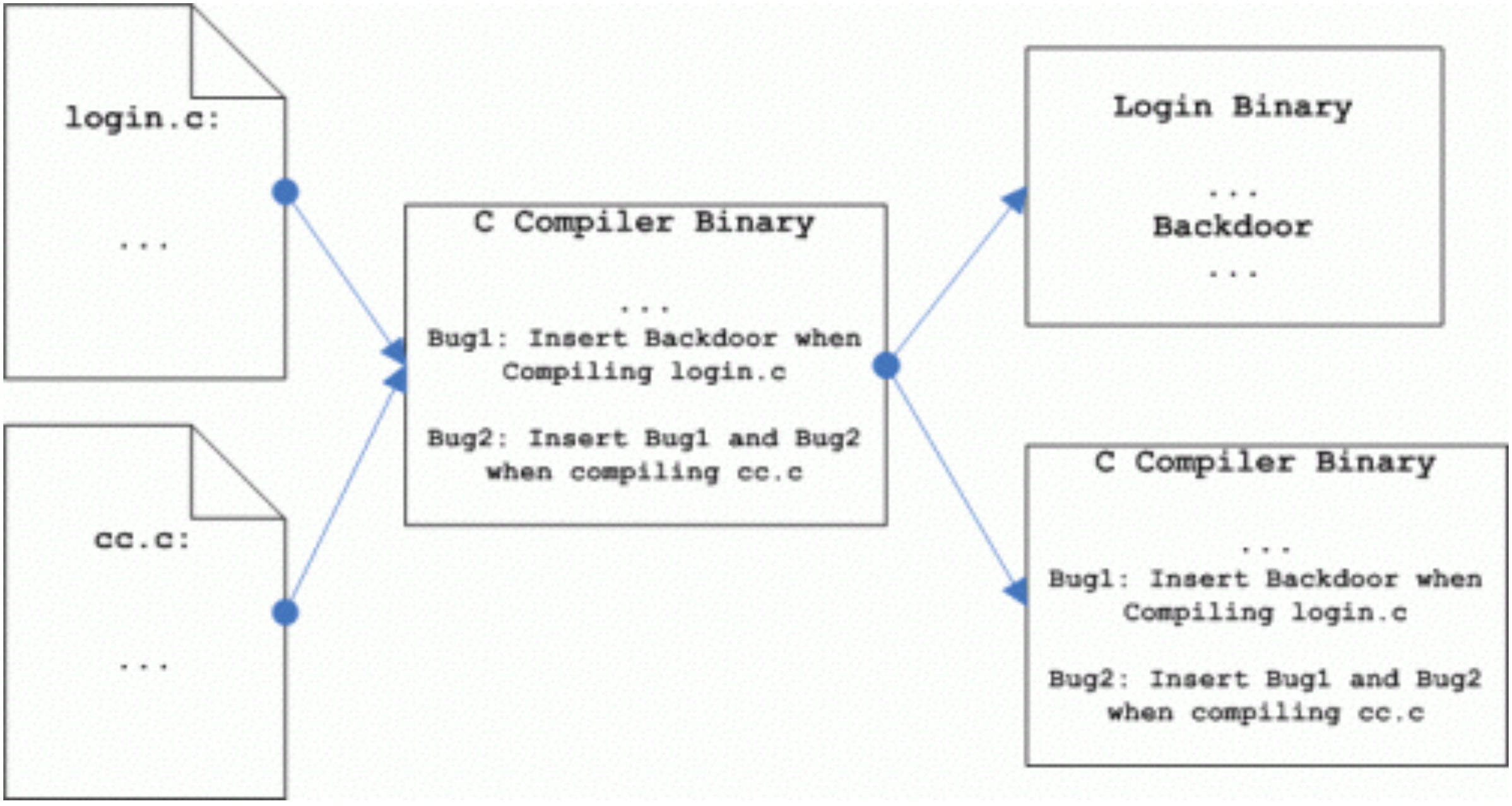
First time:

- boot into single-user mode
- generate TPM-backed CSR
- submit CSR to service in datacenter
- cert generated, used to encrypt client puppet key
- encrypted puppet key stored in host image

Nth time:

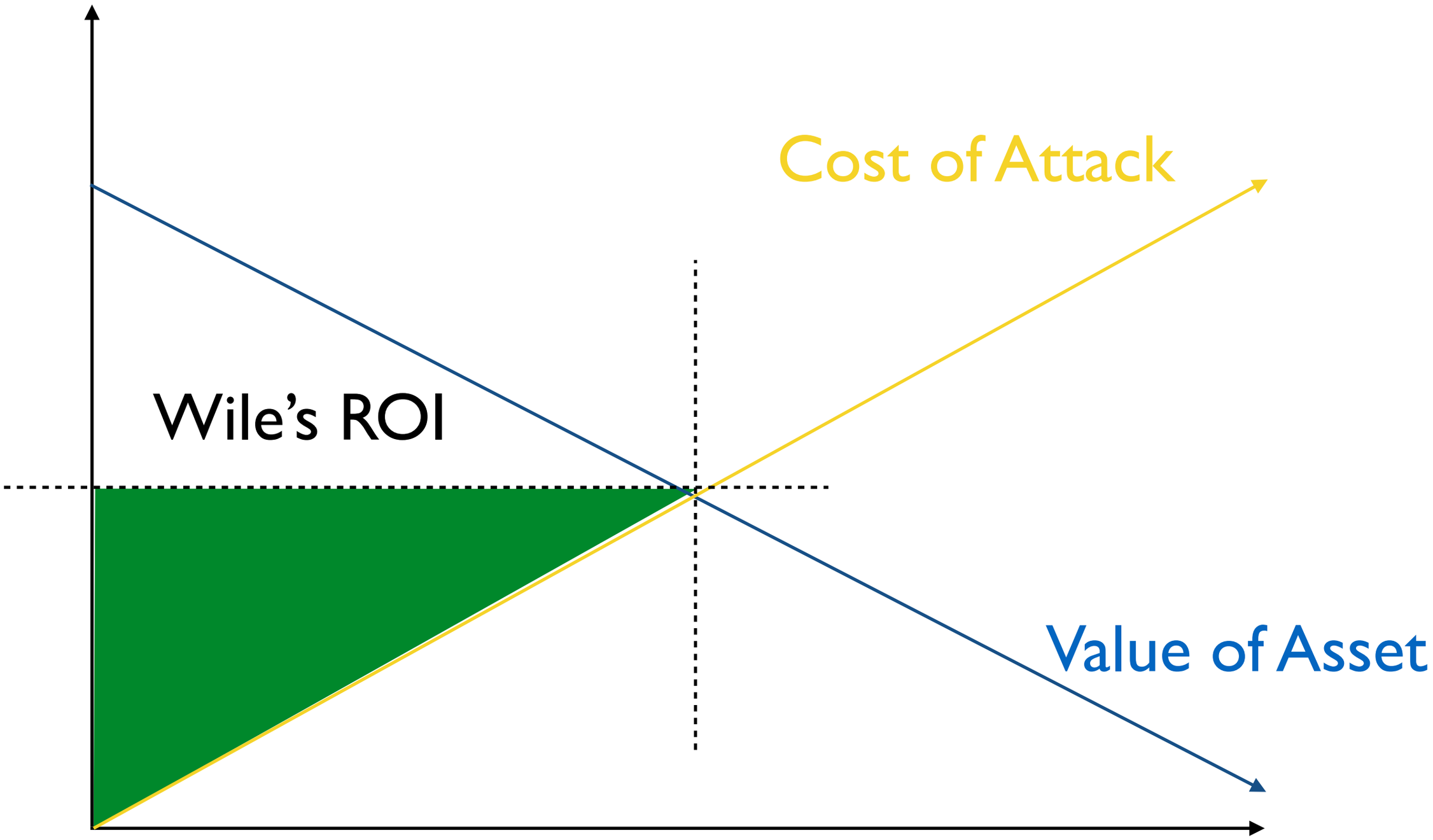
- iPXE via TLS
- `init` script decrypts puppet key using TPM
- puppet does its thing

Obligatory "Reflections on Trusting Trust" reference.

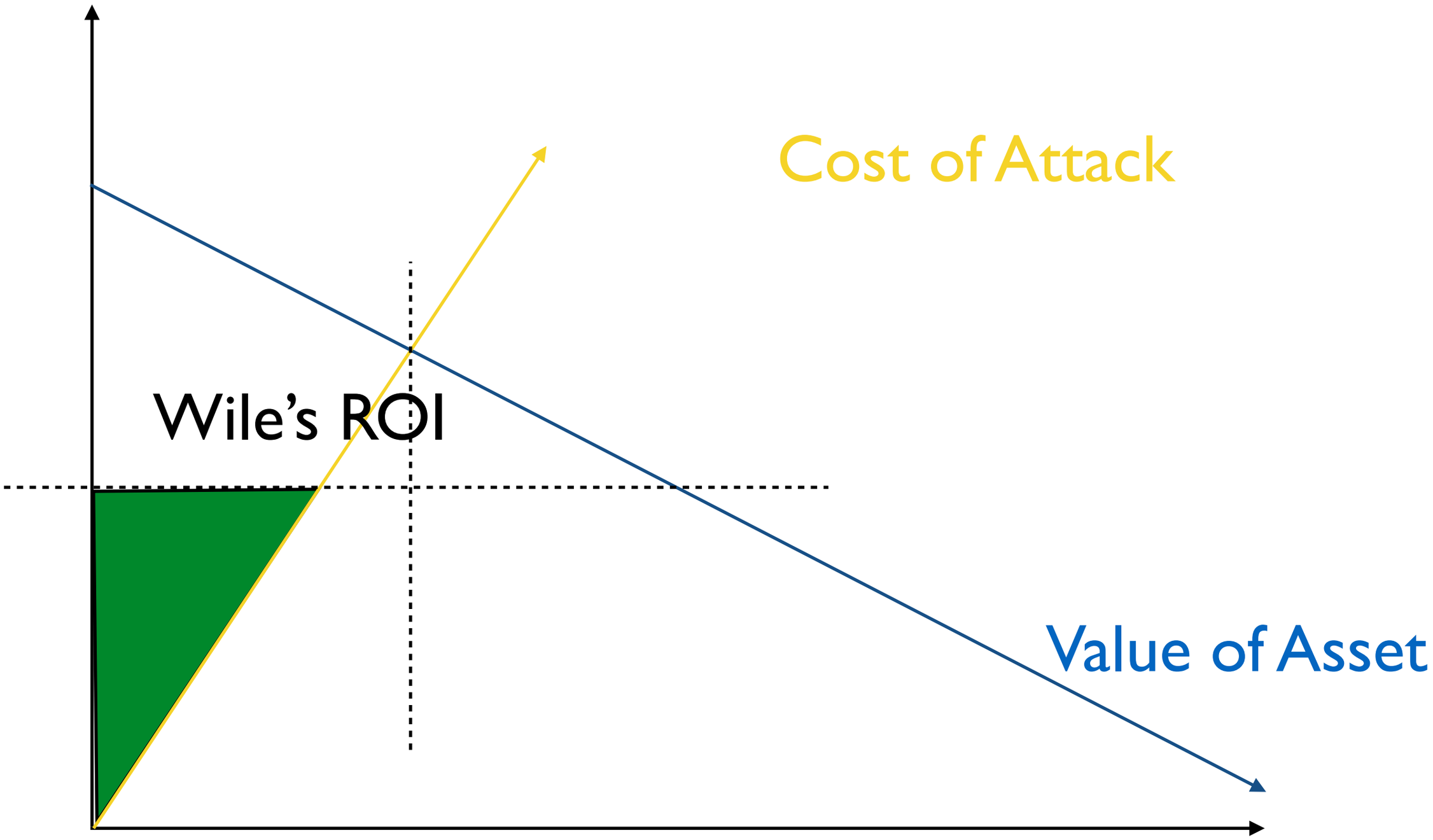



http://cm.bell-labs.com/who/ken/trust.html

# Wile E. Coyote has an MBA.



# Wile E. Coyote has an MBA.

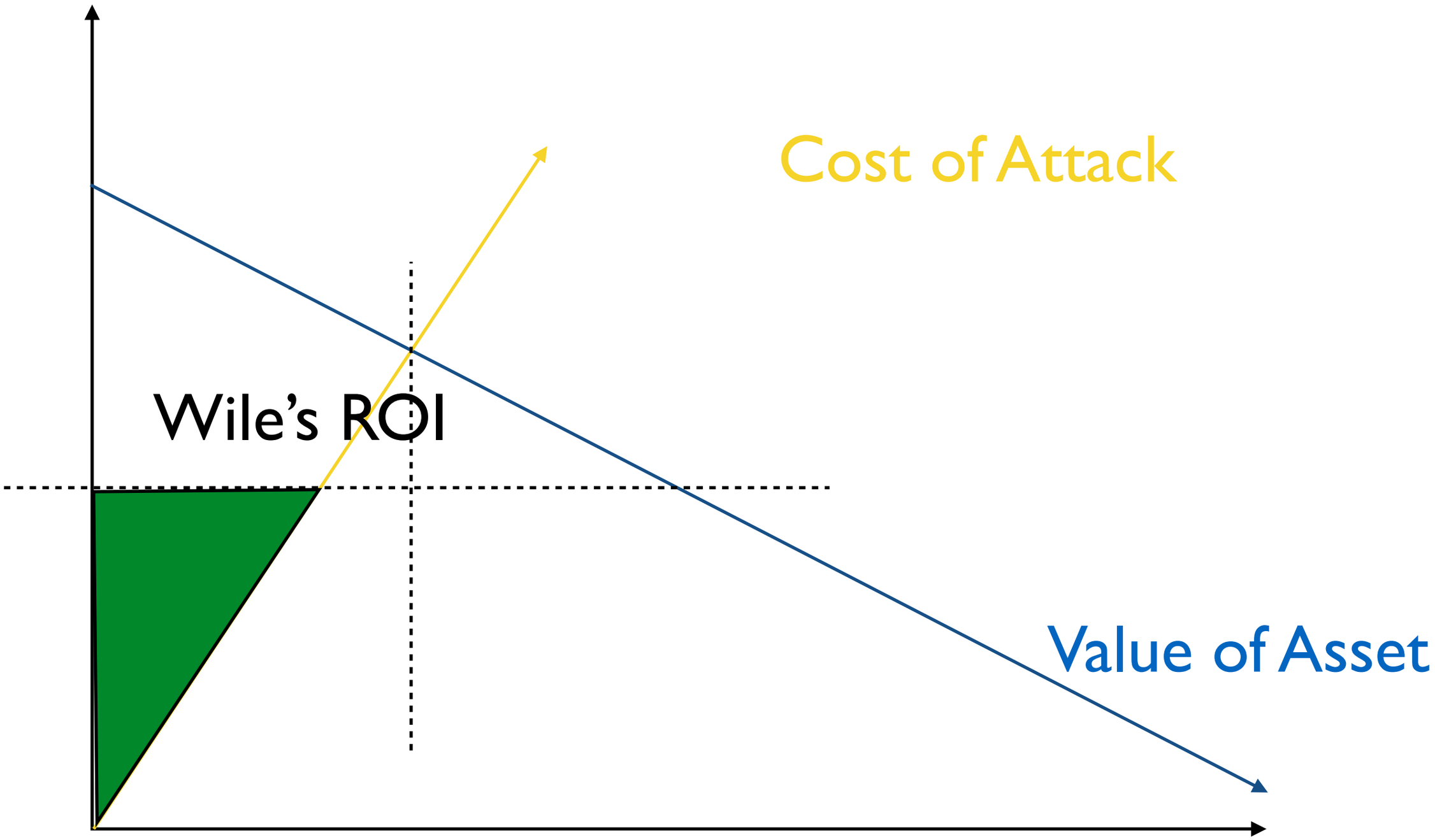



# Raising the cost of attack

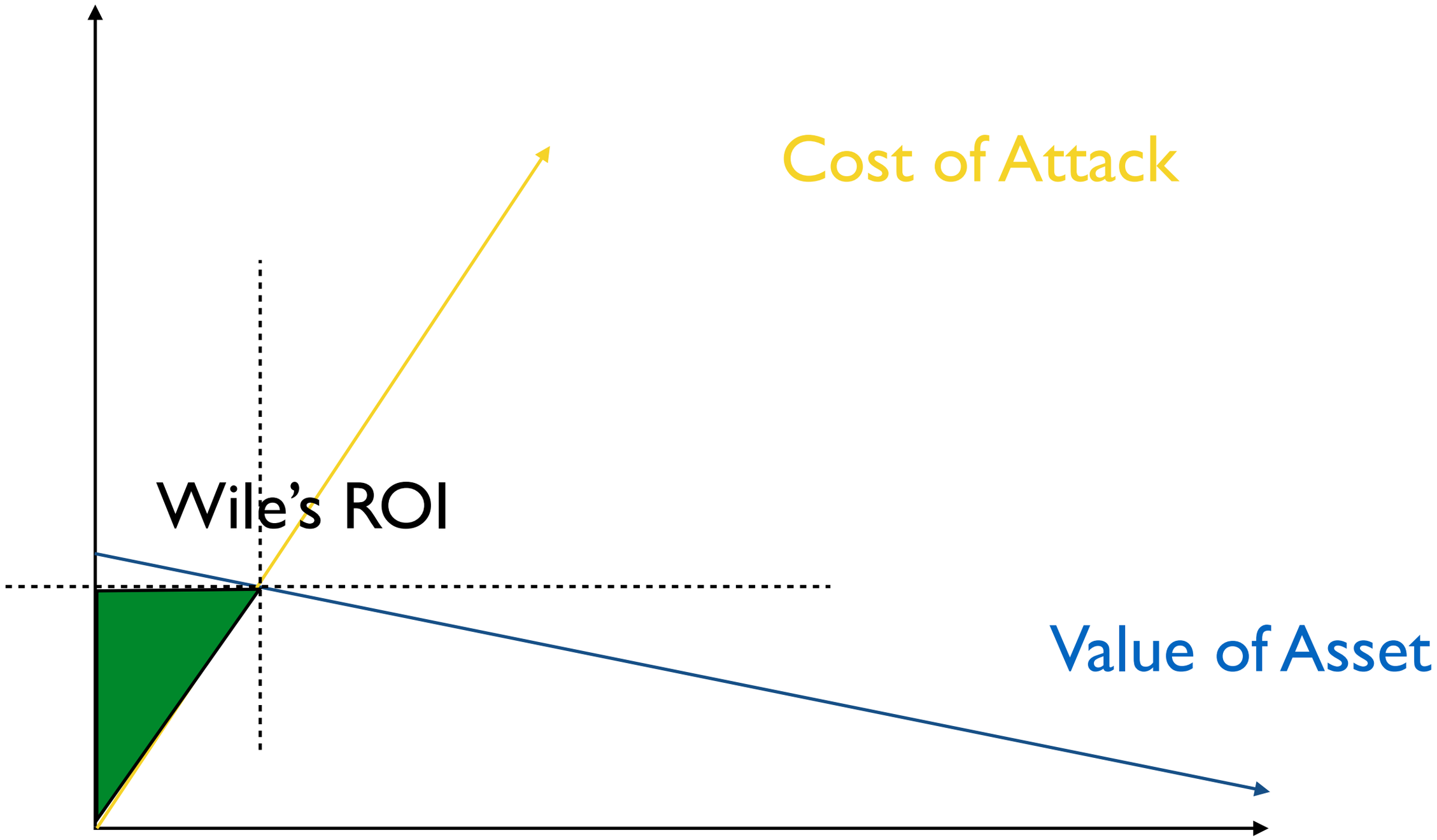
Wile E. Coyote needs:

- physical access
- ability to attack running system
- persistent undetected presence

# Wile E. Coyote has an MBA.



# Wile E. Coyote has an MBA.

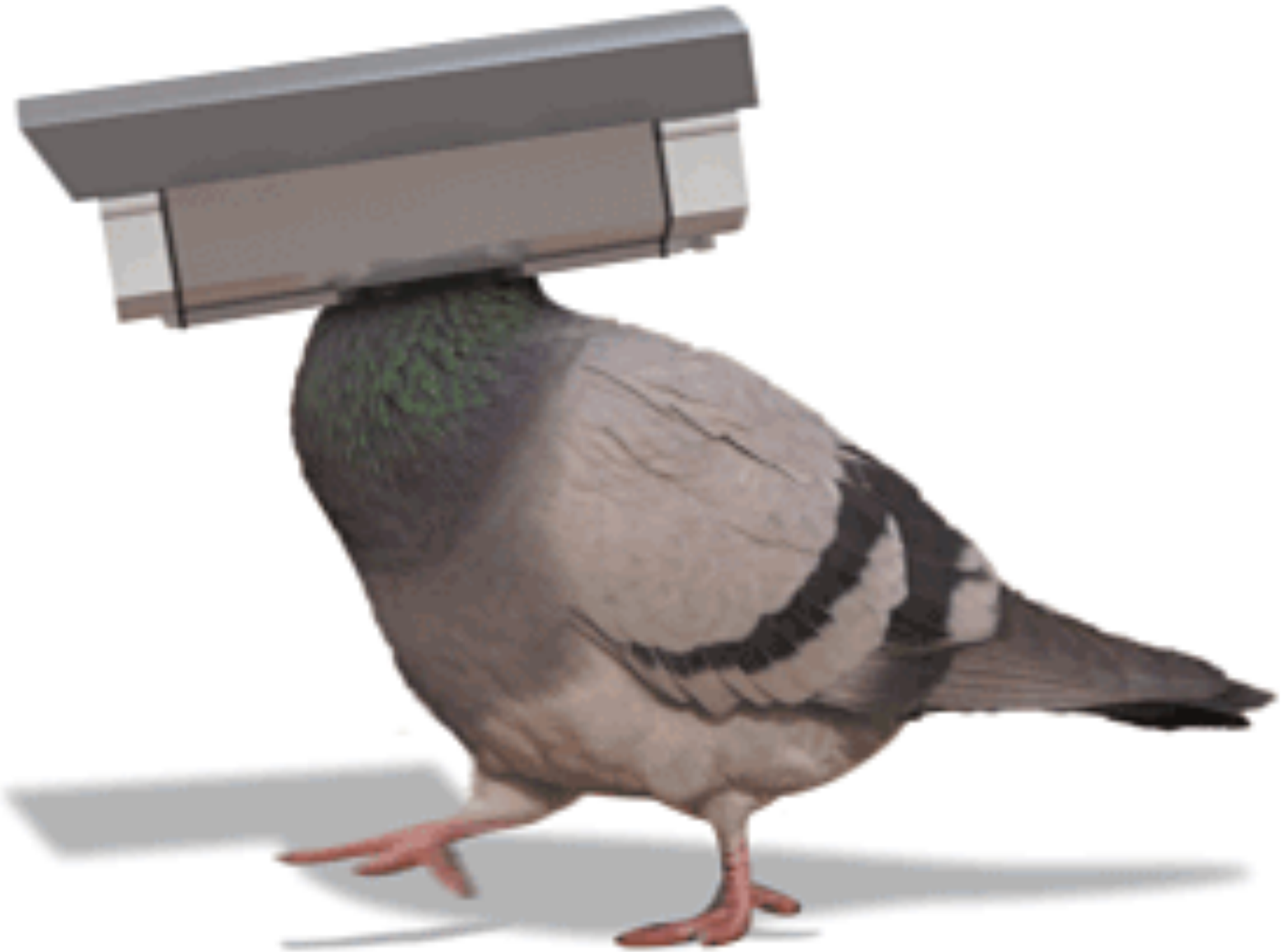


# Reducing the value of TLS keys

- Forward Secrecy
- tightly scoped certificates
- short-lived
- alert if observed outside of expected env

# Possible scenarios

- hardware compromised prior to us racking it
- resources compromised through temporary physical access (ACME backdoor)
- ACME fake hole, ACME rocket powered roller skates, ACME do-it-yourself tornado kit, ACME earthquake pills, ...

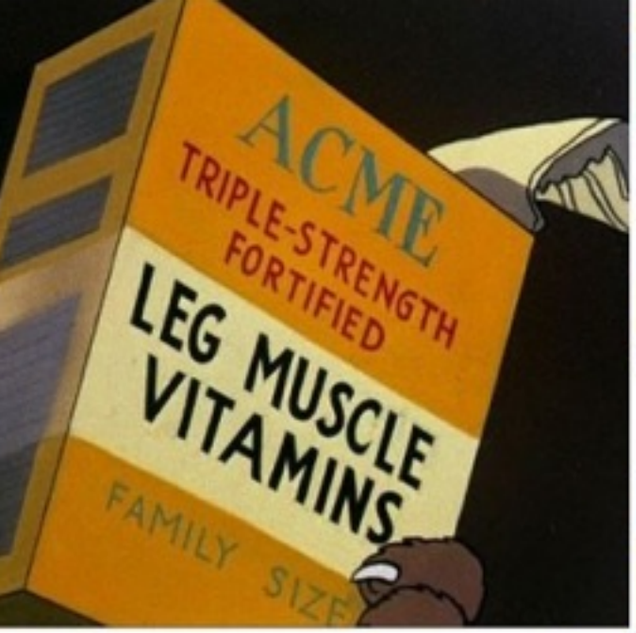


# Lessons:
# You can't just rub some crypto on it.

http://youtu.be/YsY2-yi5W74

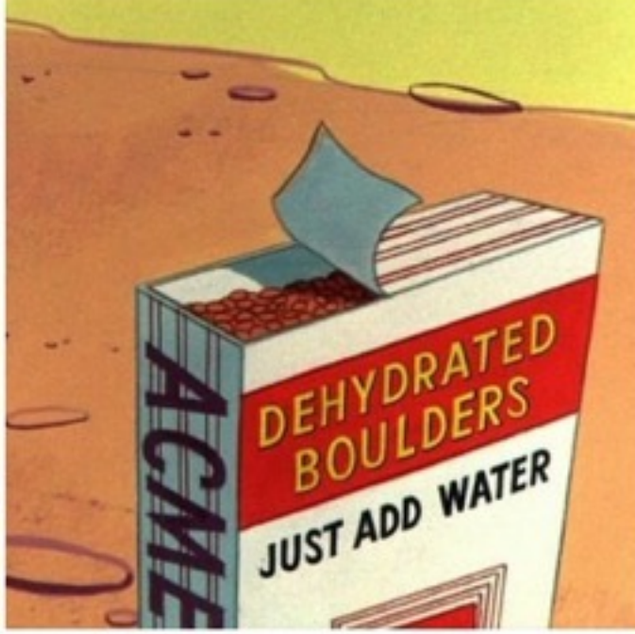
# Lessons:

# Know your assets, know your adversaries.

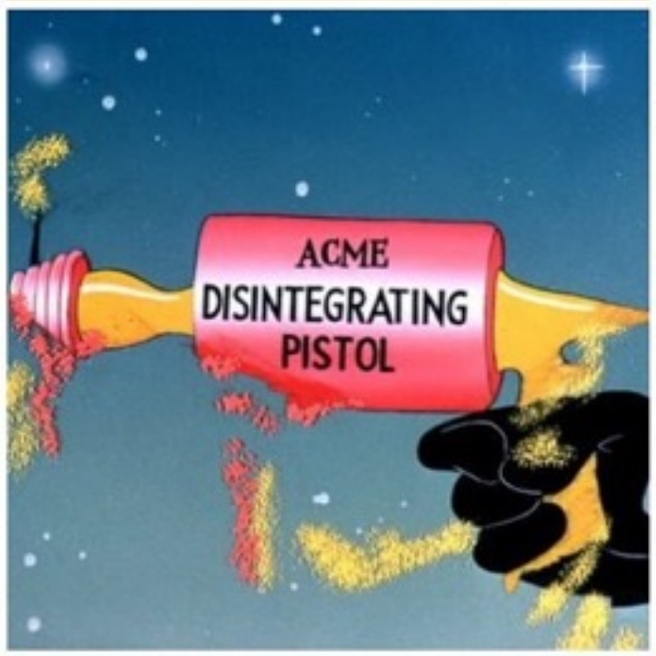

ACME
TRIPLE-STRENGTH
FORTIFIED
LEG MUSCLE
VITAMINS
FAMILY SIZE


Fleet-Foot
JET-PROPELLED
TENNIS SHOES


ONE ACME
DO-IT YOURSELF
Tornado Kit
"SEED YOUR OWN
TORNADOS"


ACME
DEHYDRATED
BOULDERS
JUST ADD WATER


ACME
EARTHQUAKE
PILLS
WHY WAIT?
MAKE YOUR OWN
EARTHQUAKES-LOADS
OF FUN!

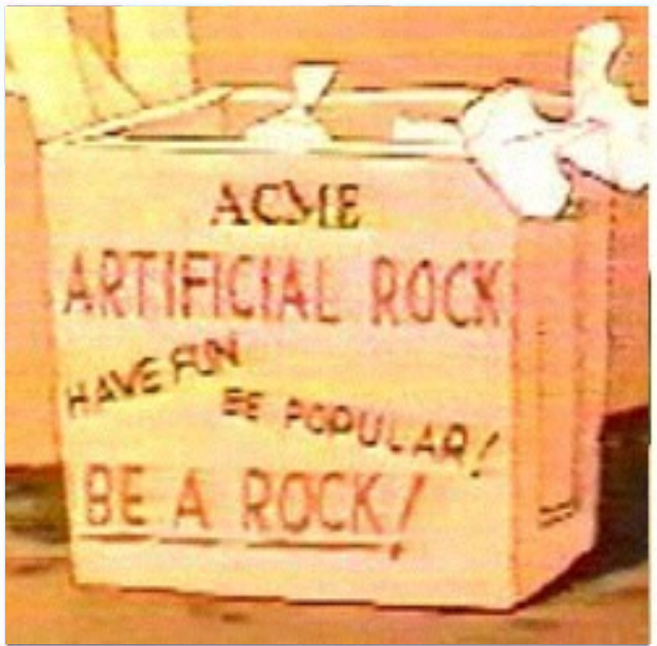

ACME
DISINTEGRATING
PISTOL


ONE
ACME
BAT-MAN'S
OUTFIT
ACME MFG. CO.
REG. SIZE

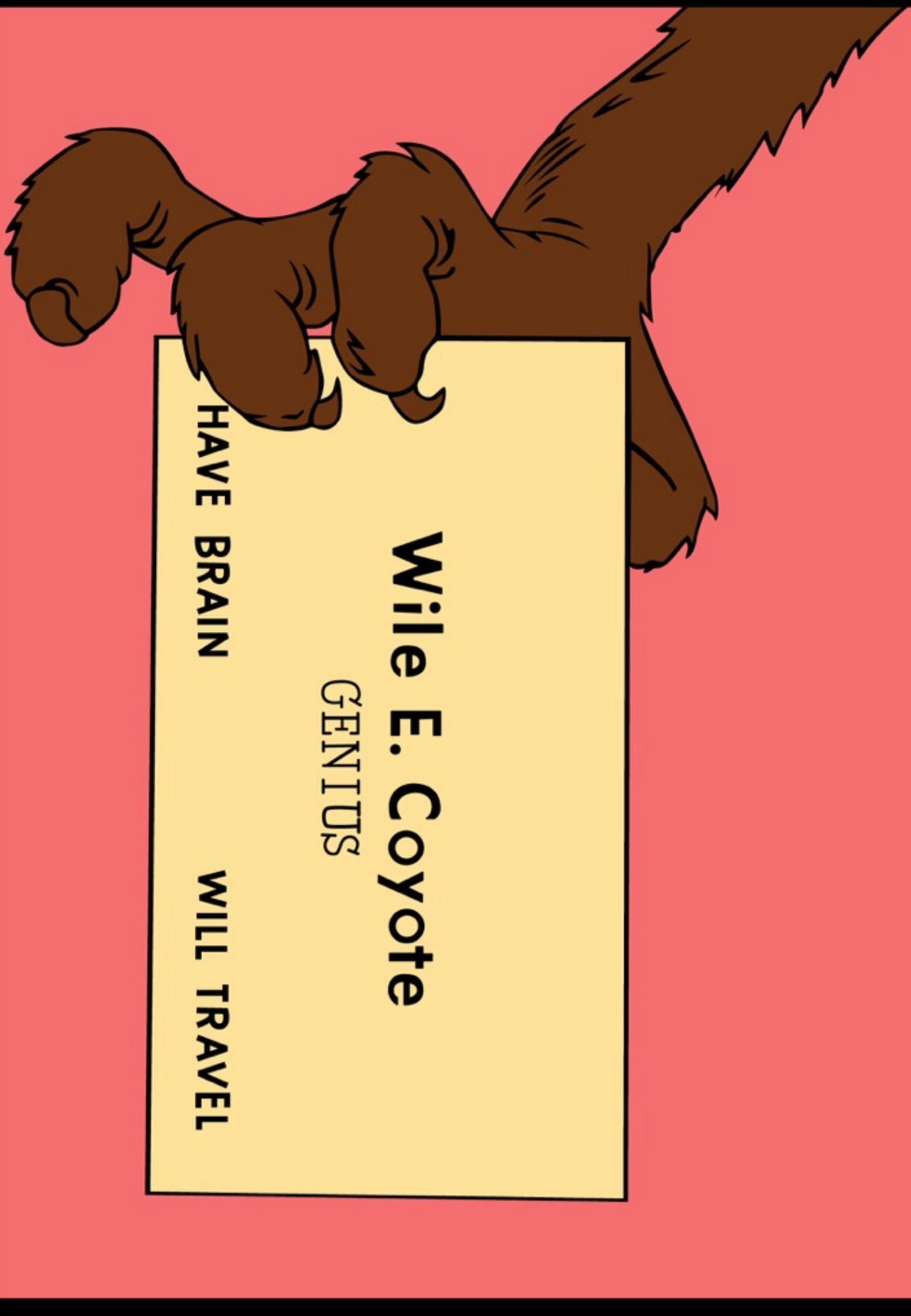

ONE
ACME
OUT-BOARD
MOTOR
ONE
JIM-DANDY
WAGON


ACME HOUSE
INSTANT
GIRL
PIERCE PHOBIAS CO.


ONE
ACME
STREET
CLEANER'S
WAGON
ONE
WEATHER
BALLOON
SELF-INFLATING
TYPE
500LB.
ANVIL
EXCELSIOR
ELECTRIC
FAN


ACME
ARTIFICIAL ROCK
HAVE FUN
BE POPULAR!
BE A ROCK!


ACME
TRICK
BONE


Wile E. Coyote
GENIUS
HAVE BRAIN
WILL TRAVEL


SHIT'S ON FIRE, YO

# Thanks!

(now get in the llama!)

Jan Schaumann
@jschauma

54FE 193F 64ED DD0B CFDE
40D6 1983 626F 1E52 3D3A