THE PAST, THE FUTURE, AND

... wait, where the hell are we now?

Hello, this is me

Disclaimer

The opinions and positions expressed herein are mine only and do not represent the views of any current or previous employer, including Intel Corporation or its affiliates.

This presentation has no intention to advertise or devalue any current or future technology.

Scripting monkey,

Malware analyst,

Reverse engineer,

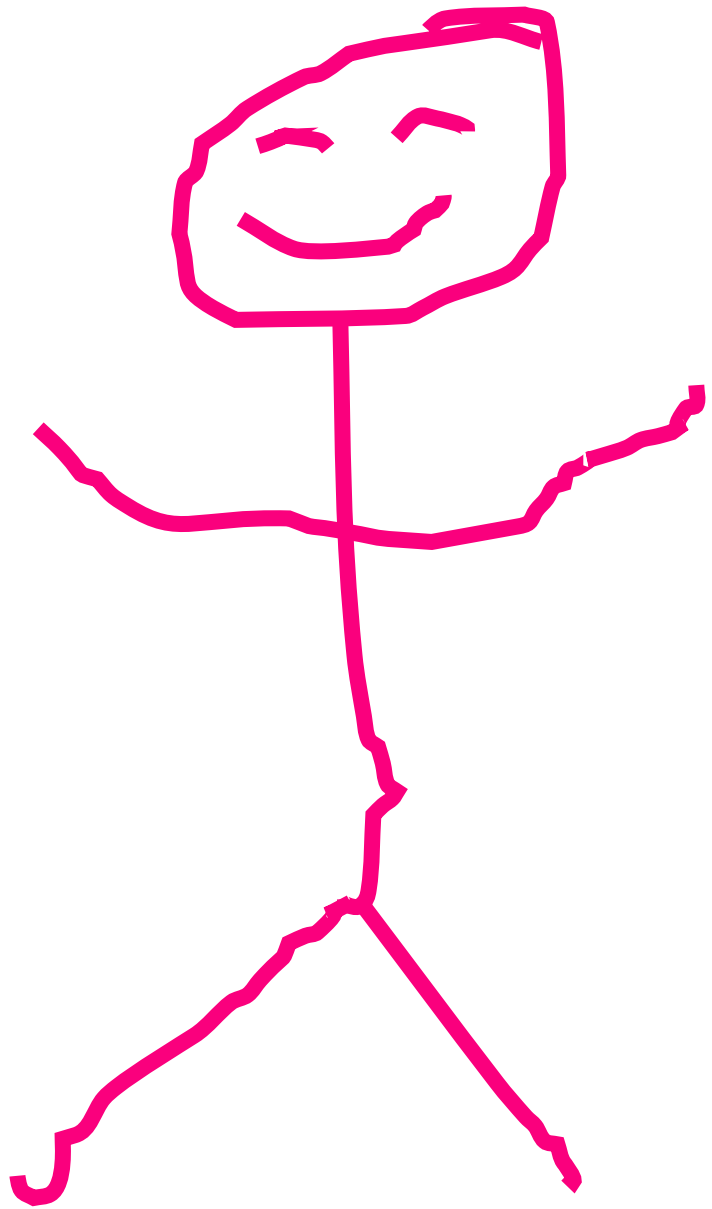
Advanced threat detection,

Nation state malware observer,

Incident response,

And then I went low level.

(HITB \m/-.-\m/)




Why


GOING LOW


WELCOME TO
FAR FAR
AWAY

We are all searching for something

Known-Bad

Known-Good

Non Known-Good

A PARADOX

Anti-virus is dead, they said.
Pattern matching is defeated, they claimed.
Then they came up with IOCs,
and stuffed them with patterns.

Spot the problem.

Businesses will business.
Scaling is hard.
Why it will always work but never does.

The Threat Detection Myth

All the wonders we could do,
if things just worked the way they should.

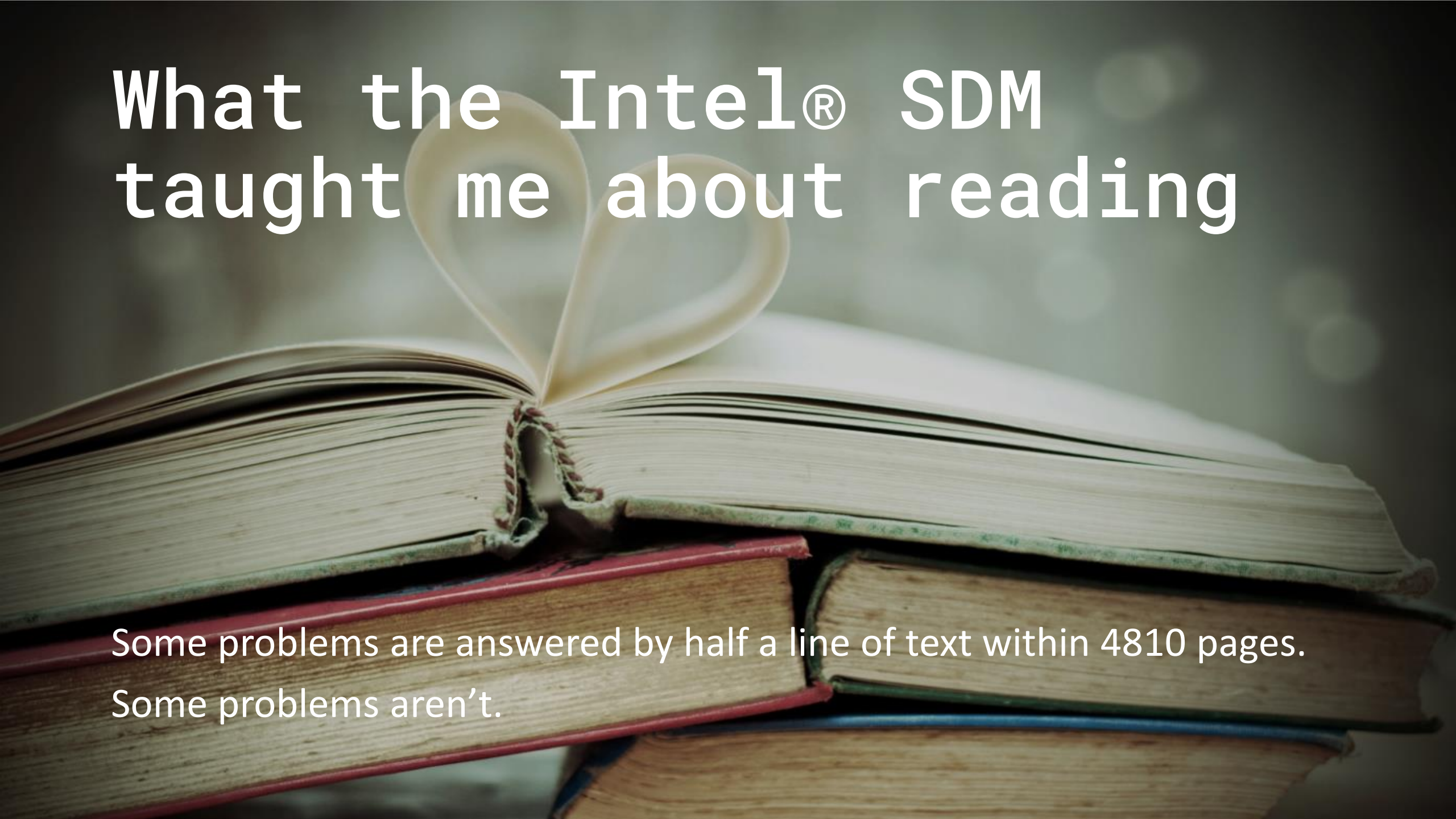
From AV to sandboxes,

from sandboxes to static analysis,

from static analysis to RE tools wonderland.

courtesy of @guedou

What the Intel® SDM taught me about reading



Some problems are answered by half a line of text within 4810 pages.

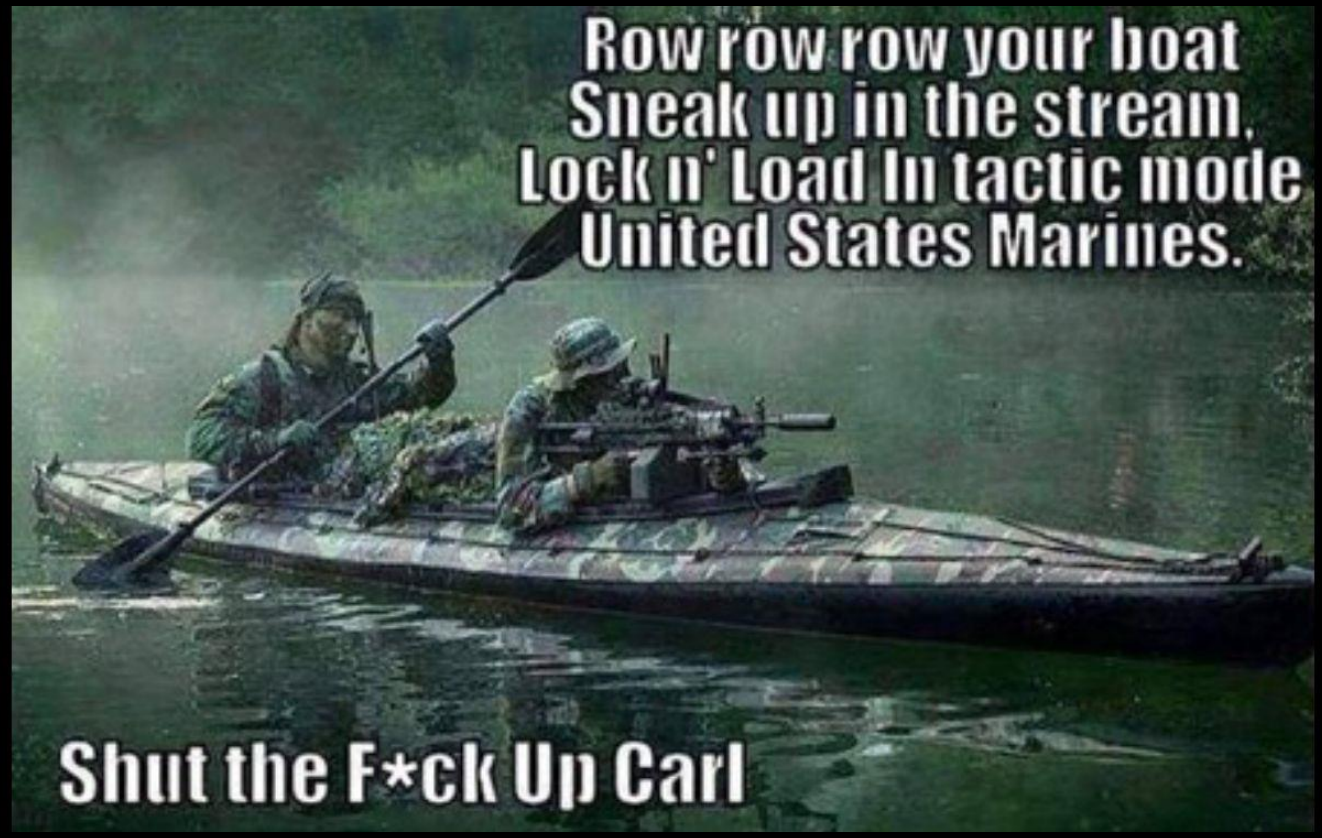
Some problems aren’t.

What conference expo halls taught me about security

My field trip into policy world and the art of nation state 1:1

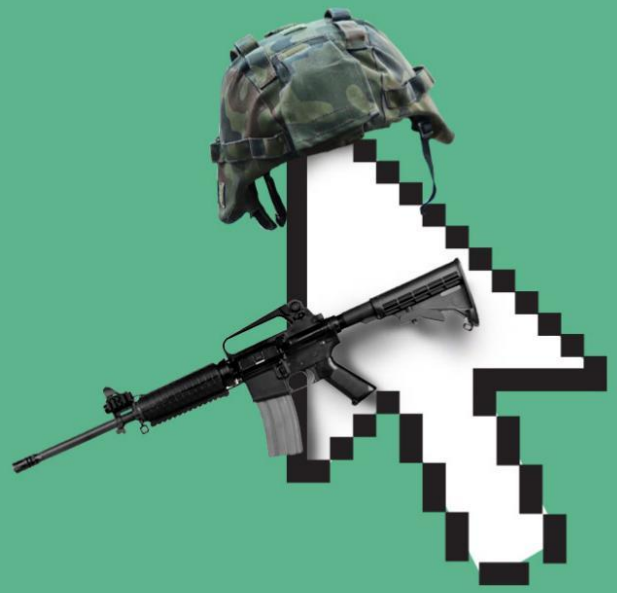
THE A AND THE P OF THE T

APT big game hunting, like Carl would



Advanced Technology Is...Advanced

What nation state malware taught me about cyber war



http://www.slate.com/articles/technology/future_tense/2016/03/are_we_headed_for_cyber_world_war_i.html

</BLANK>

fml

https://github.com/marasawr/fml

I read 20 years of mostly-fail at cyber norms at the UN, and now you can too!

How to use this repository

Organisation & naming conventions

• Files have been renamed to reflect UN document IDs rather than job numbers (which are useless); slashes and full stops are omitted

```
- e.g., A/RES/53/70 == ARES5370.pdf; A/C.1/70/PV.21 == AC170PV21.pdf; A/61/161 == A61161.pdf
```

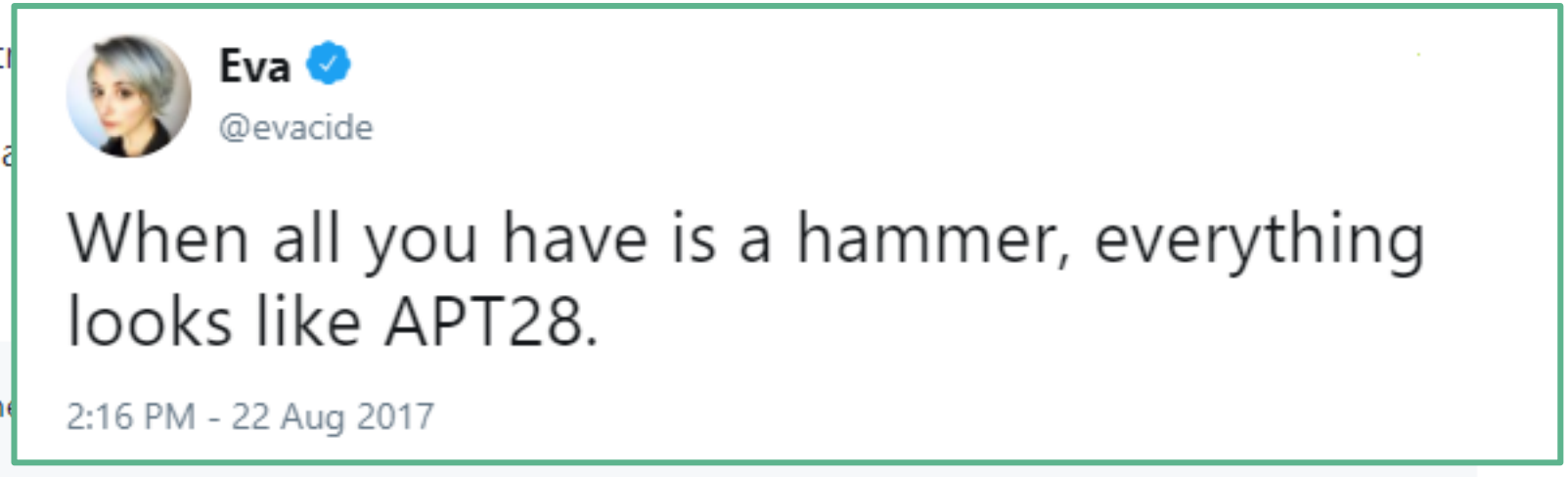
• Highlights and markups are mine; don't t

• Alternate and/or original language transl

Symbols

```
- A/ indicates a document of the Gen

- A/RES/##/### & ARES##### indicate a resolution
```



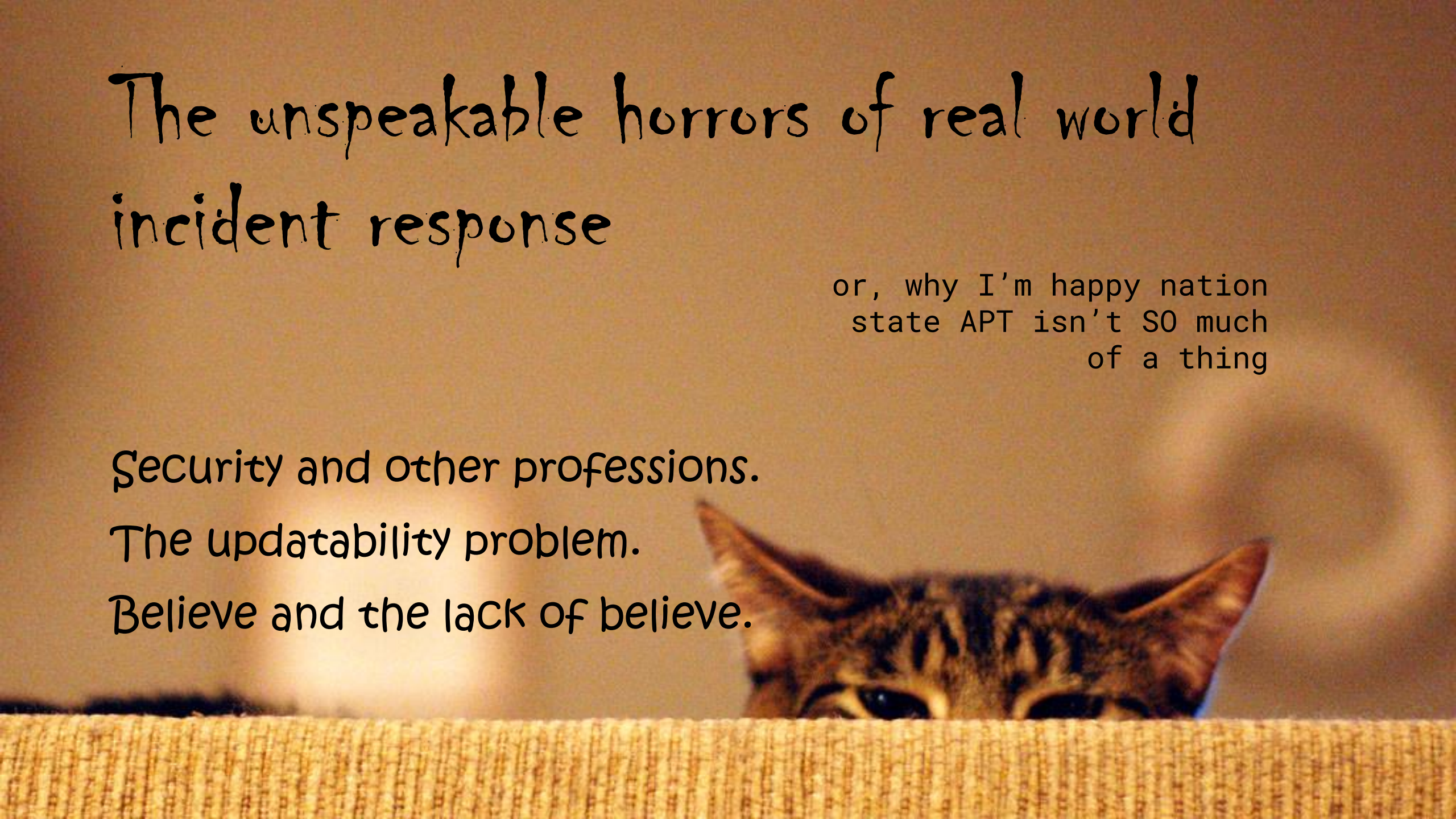
The unspeakable horrors of real world incident response

or, why I'm happy nation state APT isn't SO much of a thing

Security and other professions.

The updatability problem.

Believe and the lack of believe.



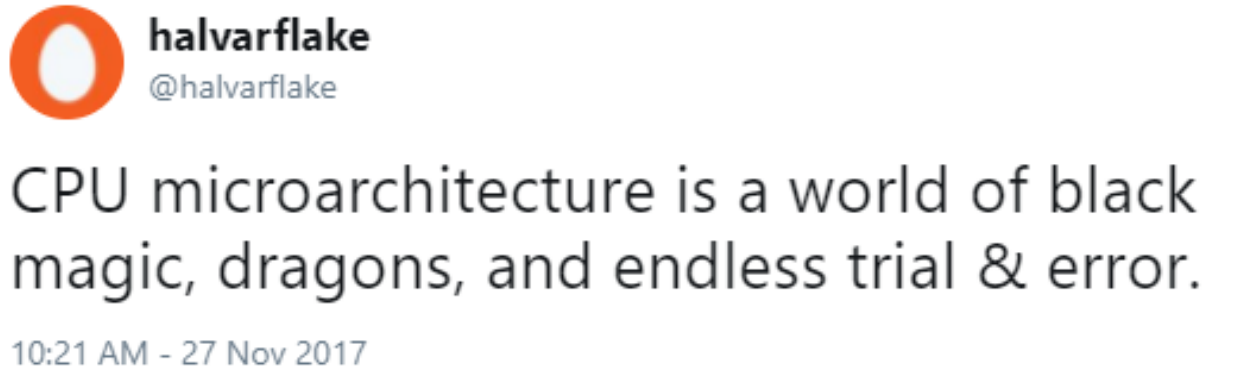
National Security

The NSA has linked the WannaCry computer worm to North Korea

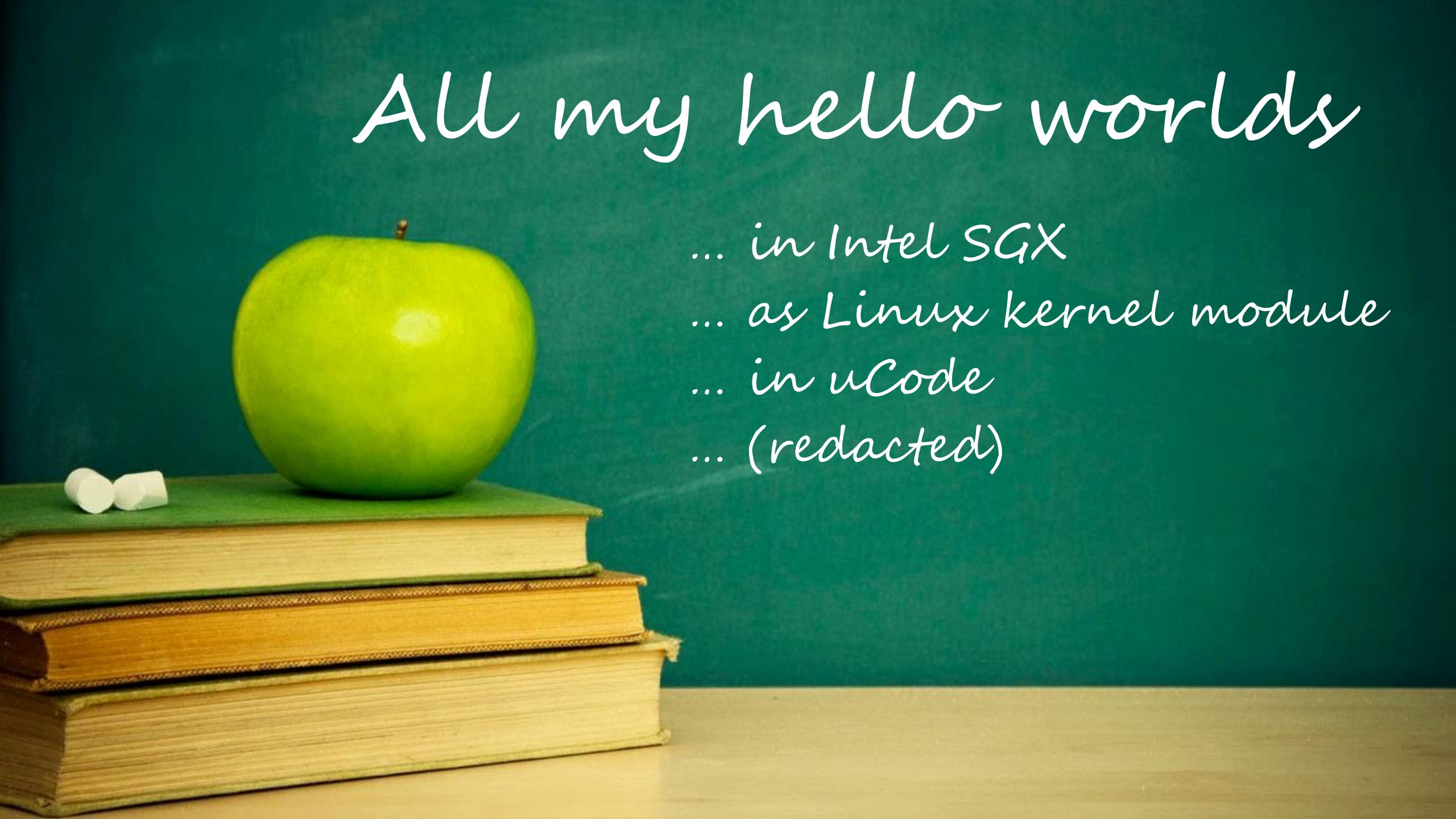
NEVERMIND.

GOING LOW

There is a world beyond x86.
Drive, guts, pain resistance.
Patience, and more patience.




.. my first bug at Intel


All my hello worlds
... in Intel SGX
... as Linux kernel module
... in uCode
... (redacted)

The meaning of growth

The only time when you are actually growing, is when you're uncomfortable

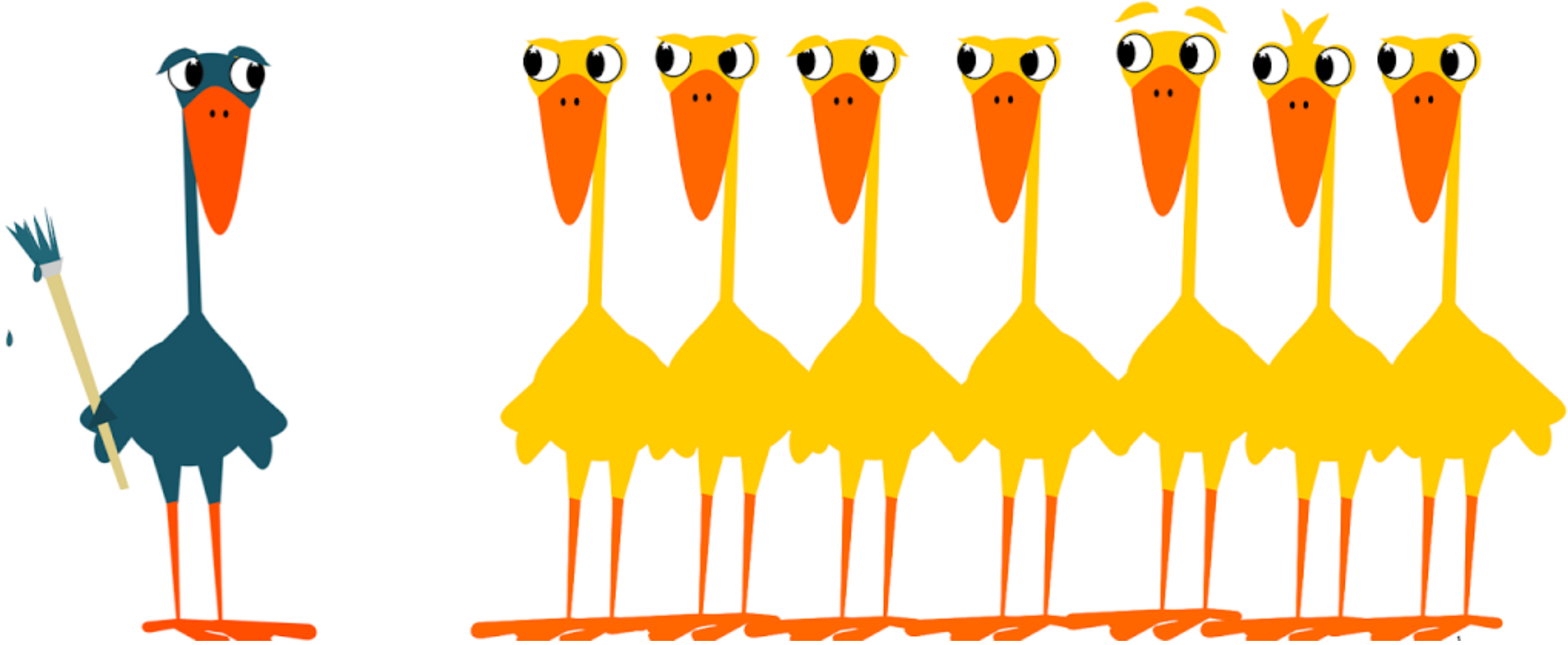
[Thomas Oppong, medium.com]

BlackHoodie

Free & women-only reverse engineering bootcamp
3 editions since 2015 - 15, 32 & 67 attendees
17 nationalities, 5 continents

As damn challenging as possible

Dunno, but
I like it...



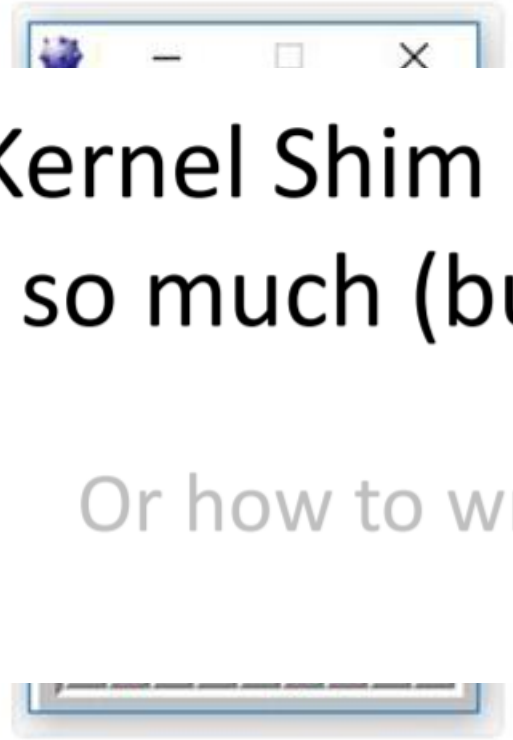
Creating Space

Pushing folks to dig deeper
.. and go further
.. and push boundaries
.. and try harder

MINORITY DRIVEN BOOTCAMPS

Ophir Harpaz
@OphirHarpaz

I just hacked Mineswe
flags on all the mined-
starting. I'm currently
person on earth.



AZERIA LABS

ARM Assembly Basics | ARM Exploitation | Lab Fundamentals | About

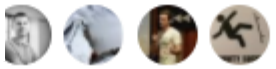
INTRODUCTION TO ARM ASSEMBLY BASICS

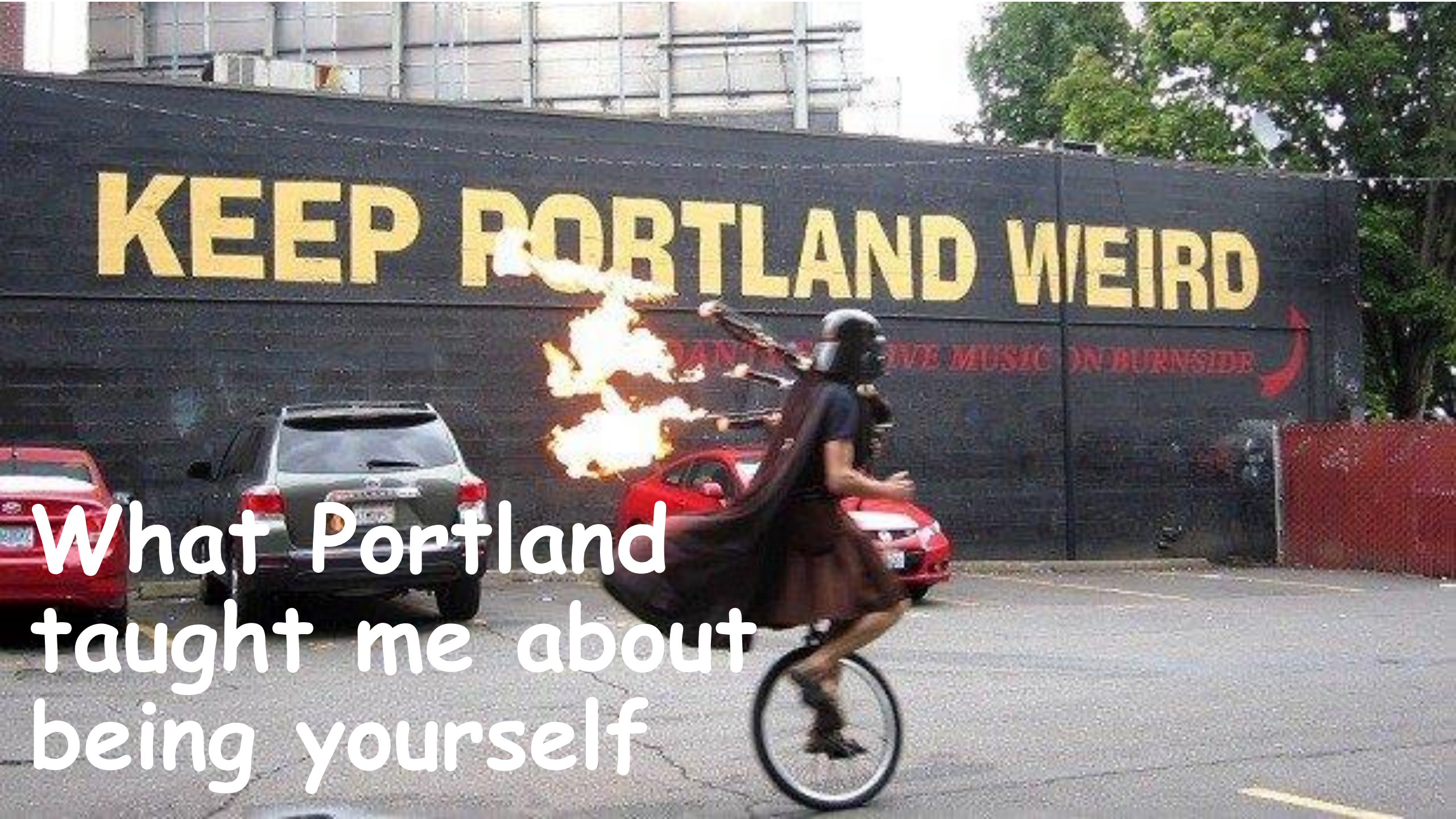
he preparation for the followup tutorial series on ARM exploit
d ROP chains, we need to cover some ARM Assembly basics first.

Kernel Shim Engine for fun and not so much (but still a little?) profit

e17 talk on flash
lable

Or how to write a super long title for nothing :)





What Portland taught me about being yourself

Thank you!