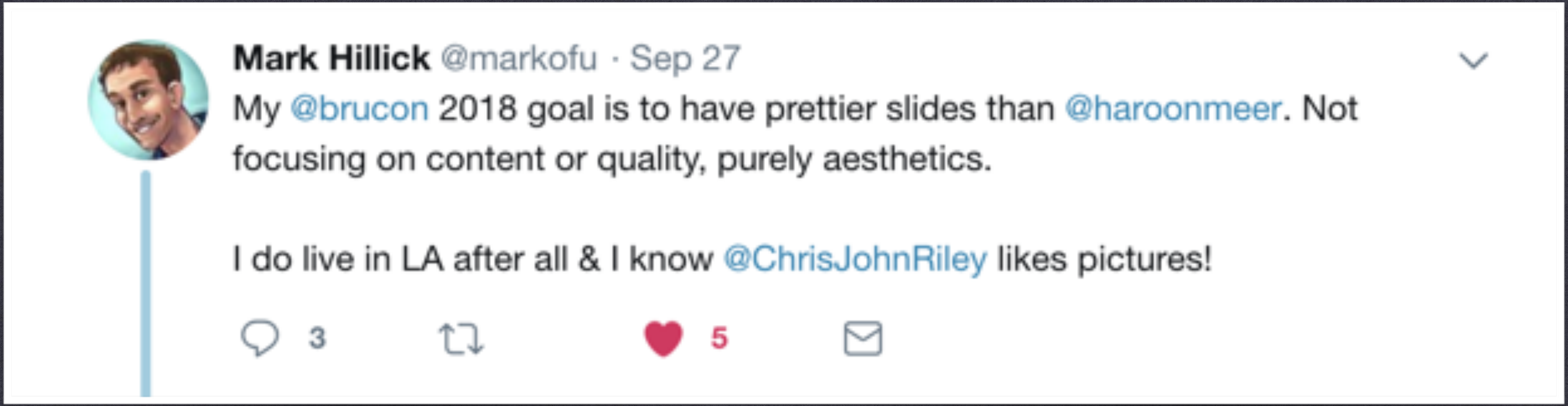
WHEN LEMON MARKETS, IMPOSTER SYNDROME AND DUNNING-KRUGER COLLIDE

@haroonmeer



Mark Hillick @markofu · Sep 27

My @brucon 2018 goal is to have prettier slides than @haroonmeer. Not focusing on content or quality, purely aesthetics.

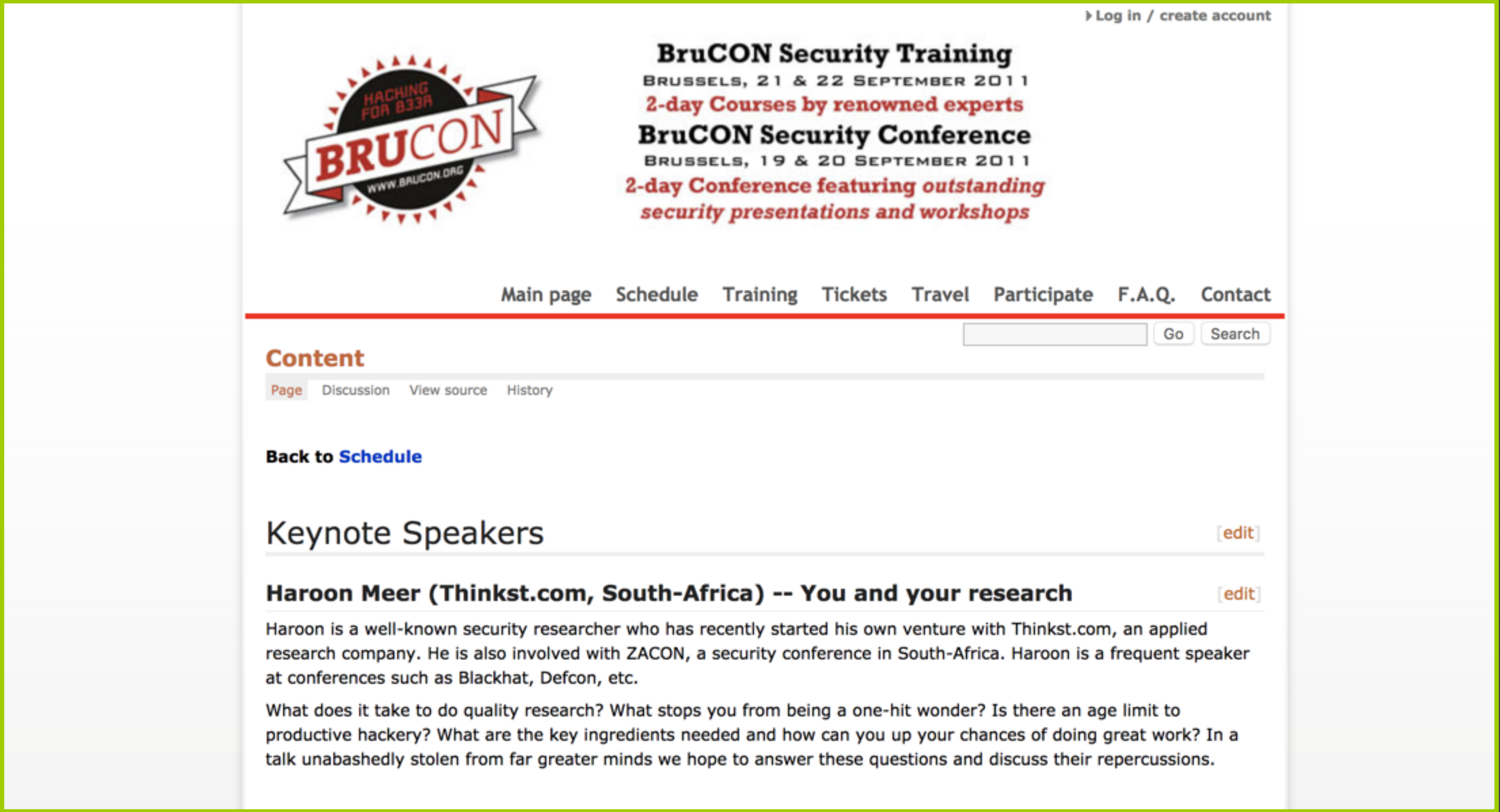
I do live in LA after all & I know @ChrisJohnRiley likes pictures!

RESTECP!

AGENDA

- Who
- 2015
- 2018
- Getting to the Nexus

Thanks!



BruCON Security Training

BRUSSELS, 21 & 22 SEPTEMBER 2011

2-day Courses by renowned experts

BruCON Security Conference

BRUSSELS, 19 & 20 SEPTEMBER 2011

2-day Conference featuring *outstanding security presentations and workshops*

Content

Back to Schedule

Keynote Speakers

Haroon Meer (Thinkst.com, South-Africa) -- You and your research

Haroon is a well-known security researcher who has recently started his own venture with Thinkst.com, an applied research company. He is also involved with ZACON, a security conference in South-Africa. Haroon is a frequent speaker at conferences such as Blackhat, Defcon, etc.

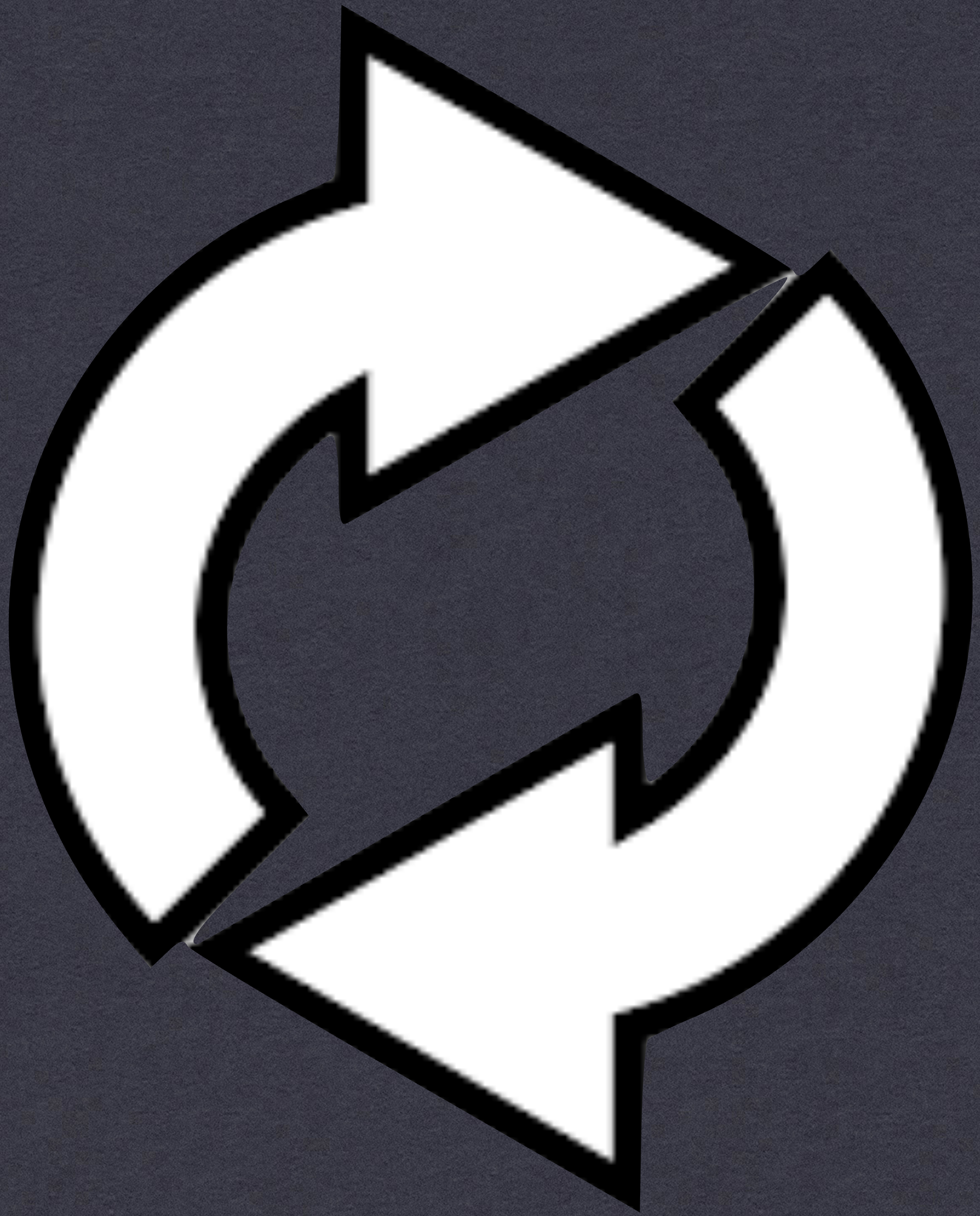
What does it take to do quality research? What stops you from being a one-hit wonder? Is there an age limit to productive hackery? What are the key ingredients needed and how can you up your chances of doing great work? In a talk unabashedly stolen from far greater minds we hope to answer these questions and discuss their repercussions.

Thanks!

Thanks x 2

Thanks!

Disclaimers



“Fig Leaf Security”

@haroonmeer - 2011

Learning the wrong lessons from Offense

@haroonmeer

thinkst
applied research

You & Your Research

2011- @haroonmeer
(haroon@thinkst.com)

Disclaimers

OLD MAN YELLS AT CLOUD

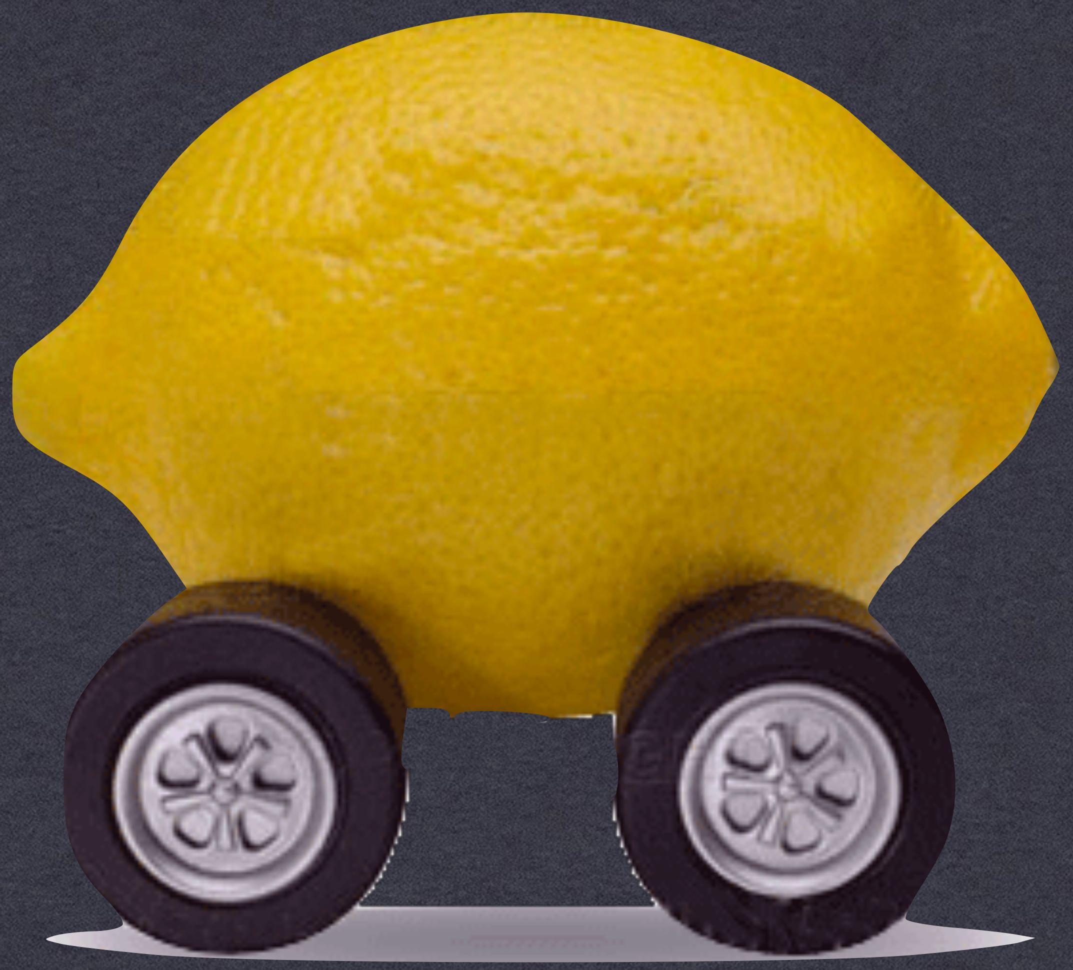
When Lemon Markets, Imposter Syndrome and Dunning-Kruger Collide

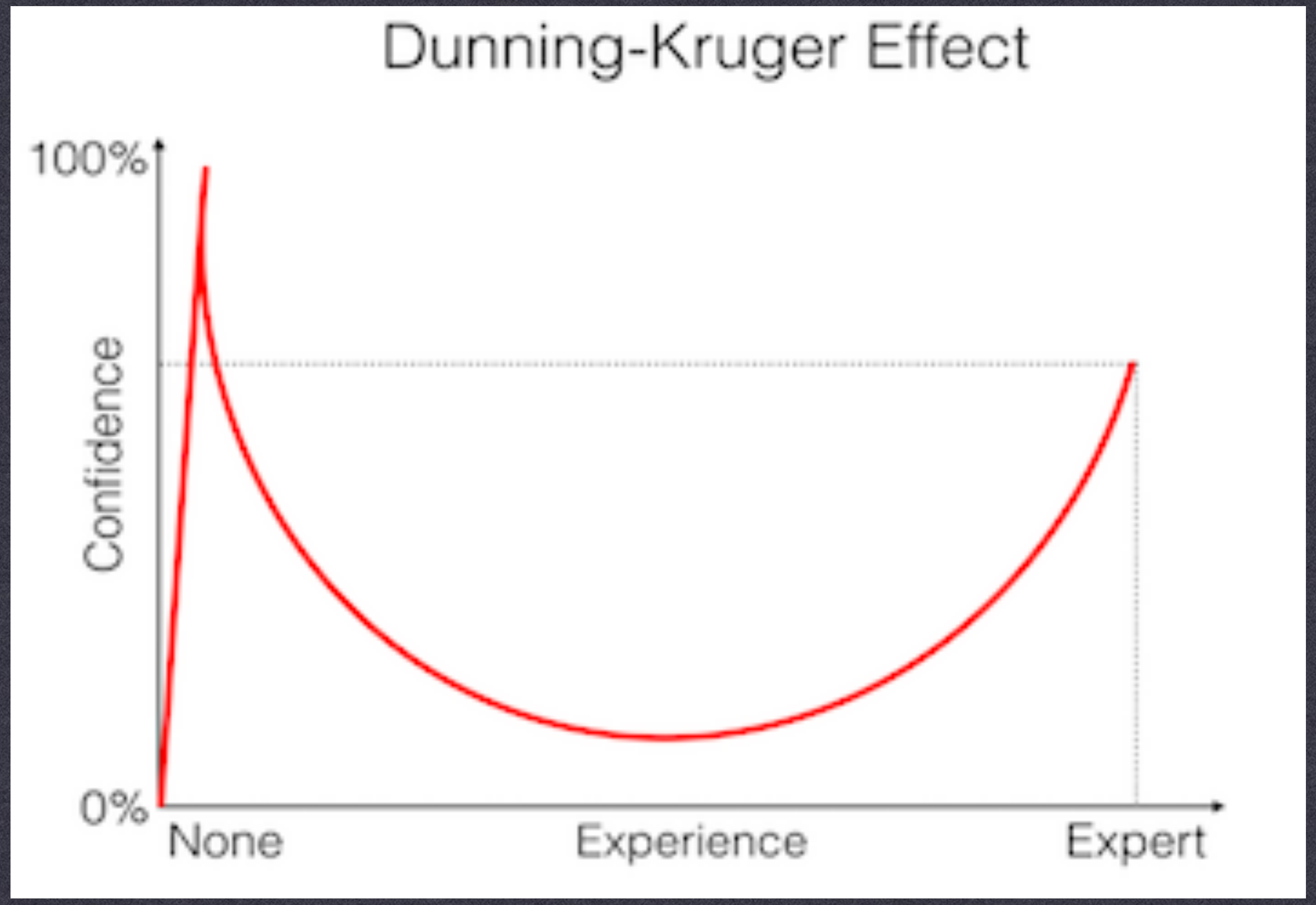
When Lemon Markets, Impostor Syndrome and Dunning-Kruger Collide

TED

~~When Lemon Markets, Imposter Syndrome and Dunning-Kruger Collide~~

Don’t be that guy!





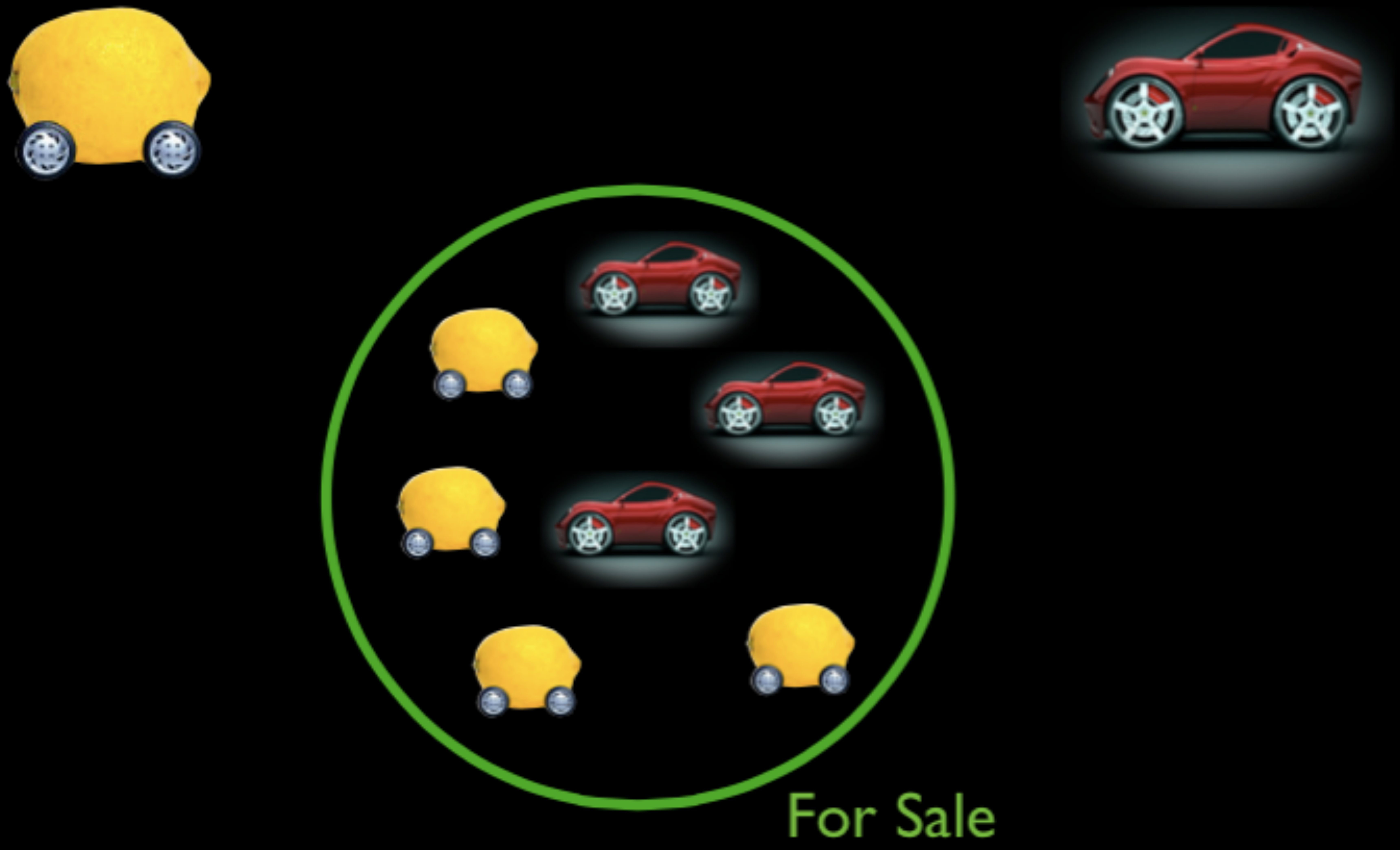
All these people really seem to have it together, and I still have no idea what's going on.

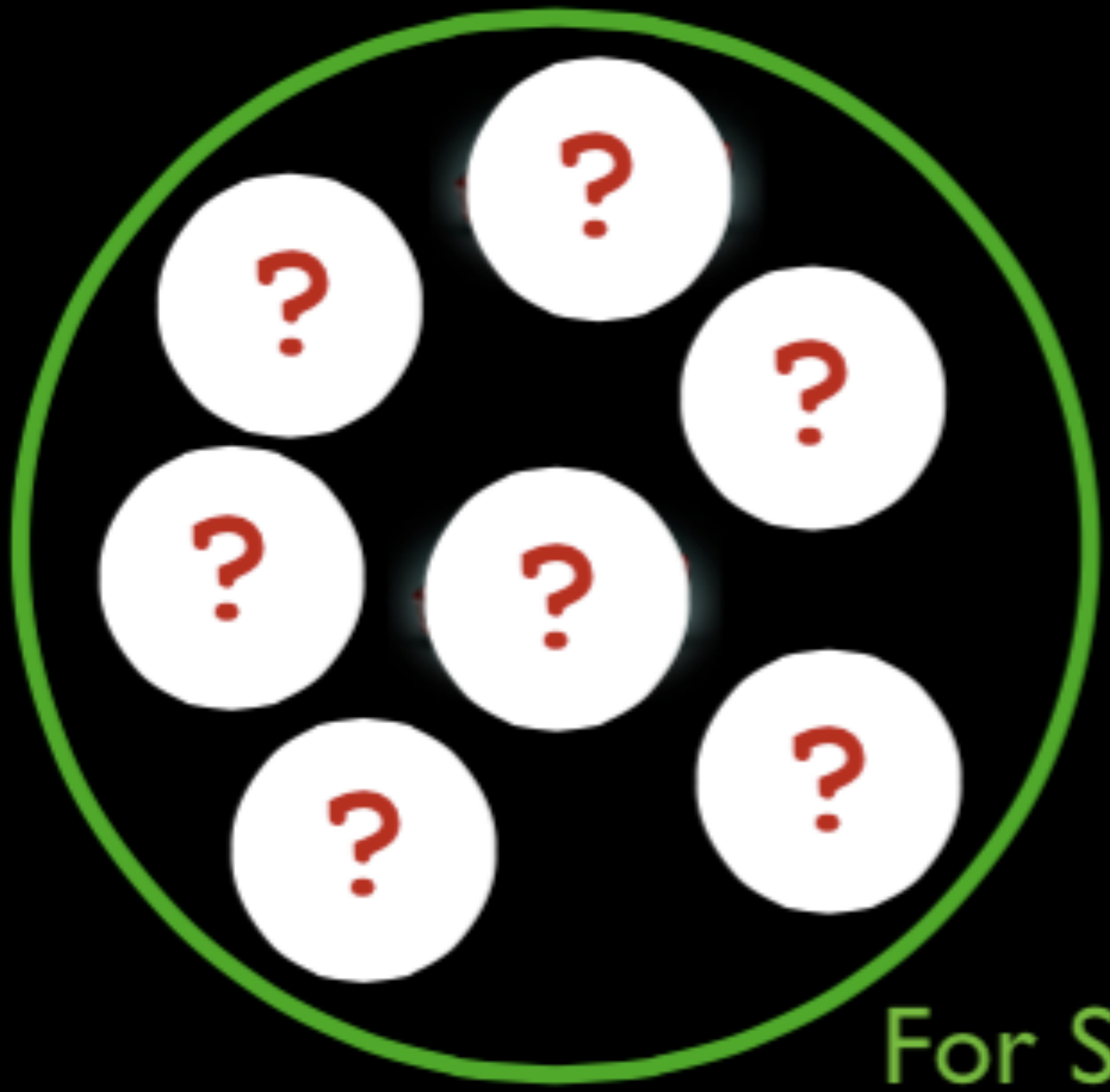
azilliondollarscomics.com

Lemon Markets

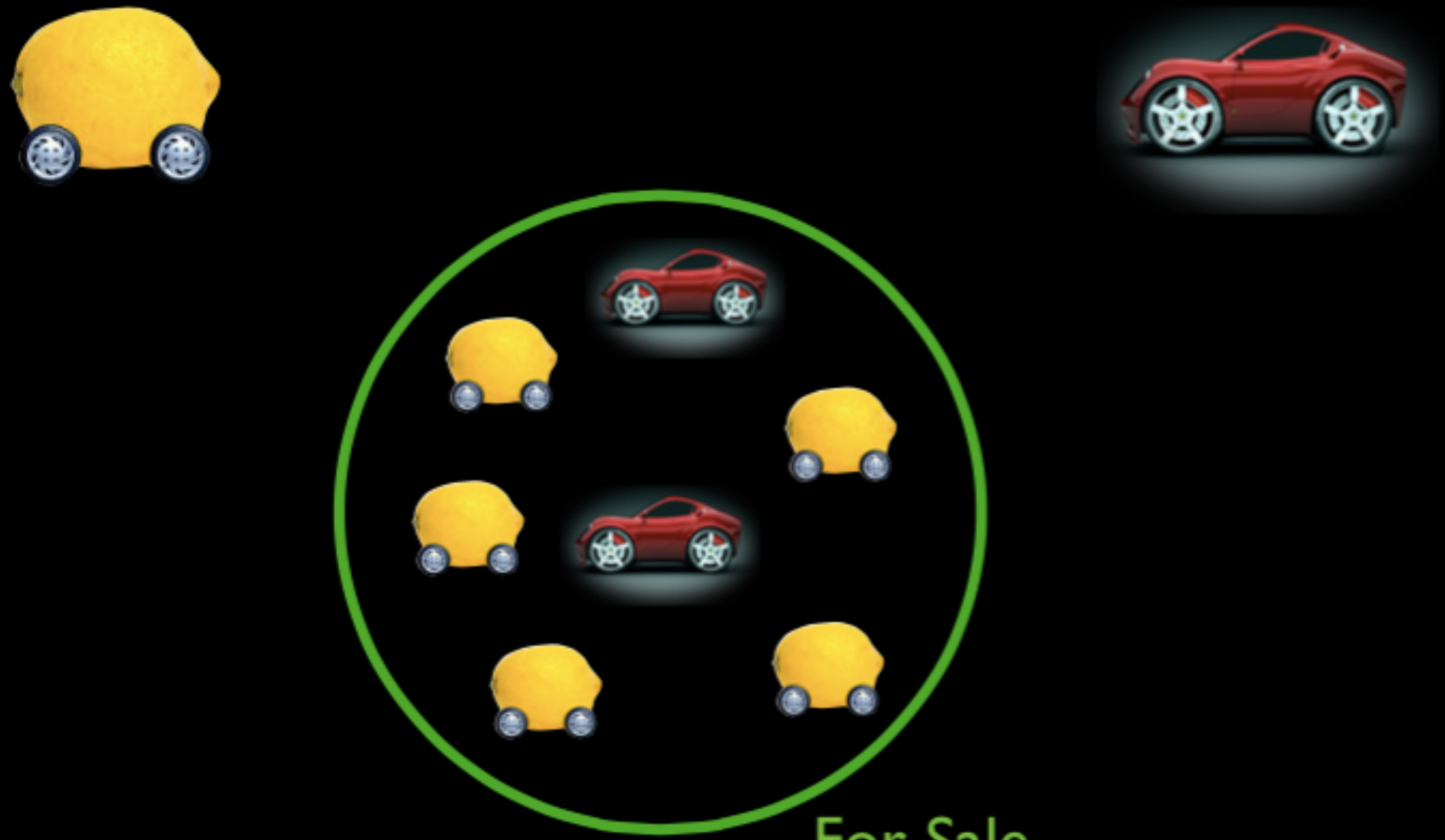
Pen-Testing Companies
a "market for lemons"

http://hydrogen.its.ucdavis.edu/eec/education/EEC-classes/eeclimate/class-readings/akerlof-the%20market%20for%20lemons.pdf

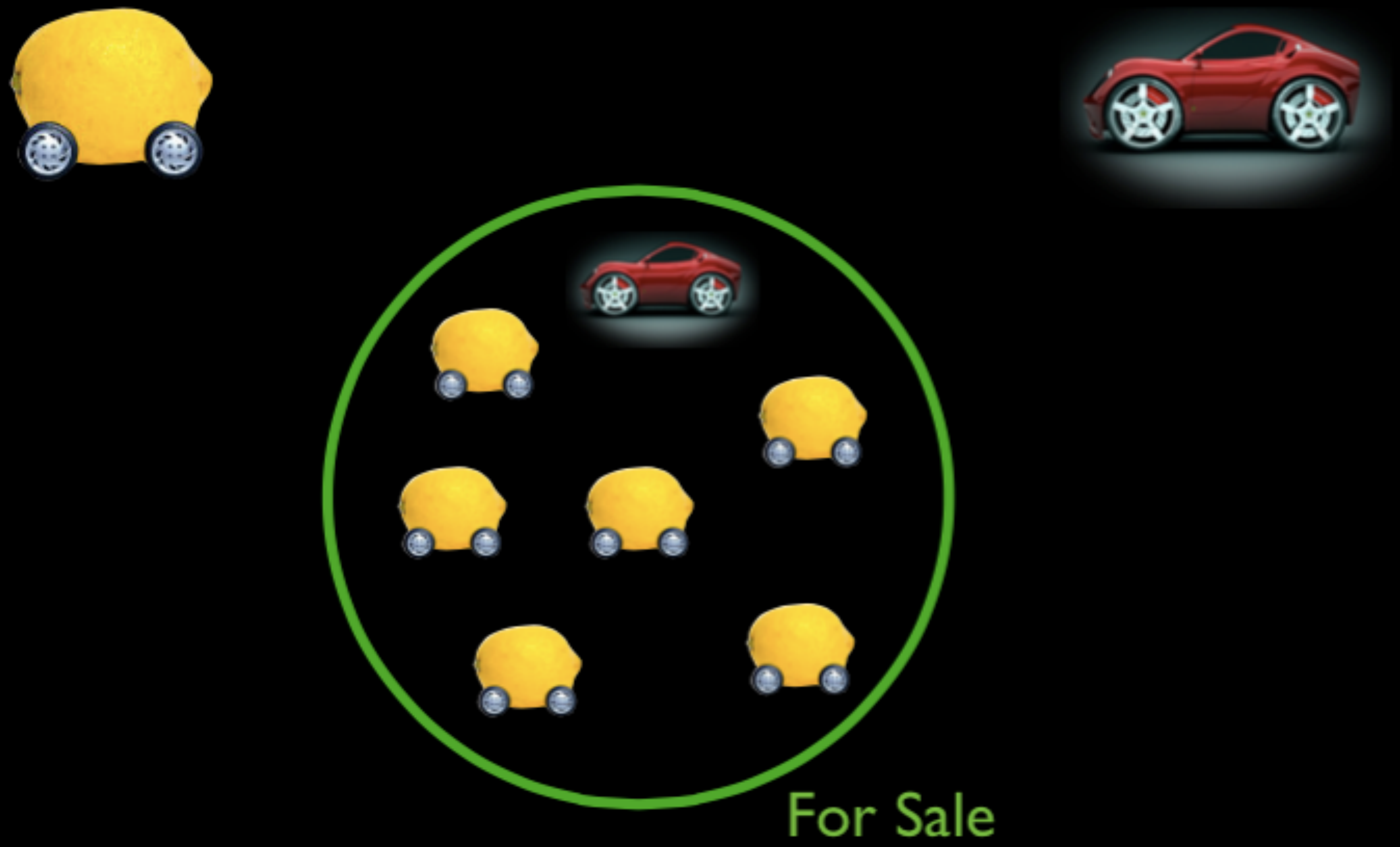

For Sale



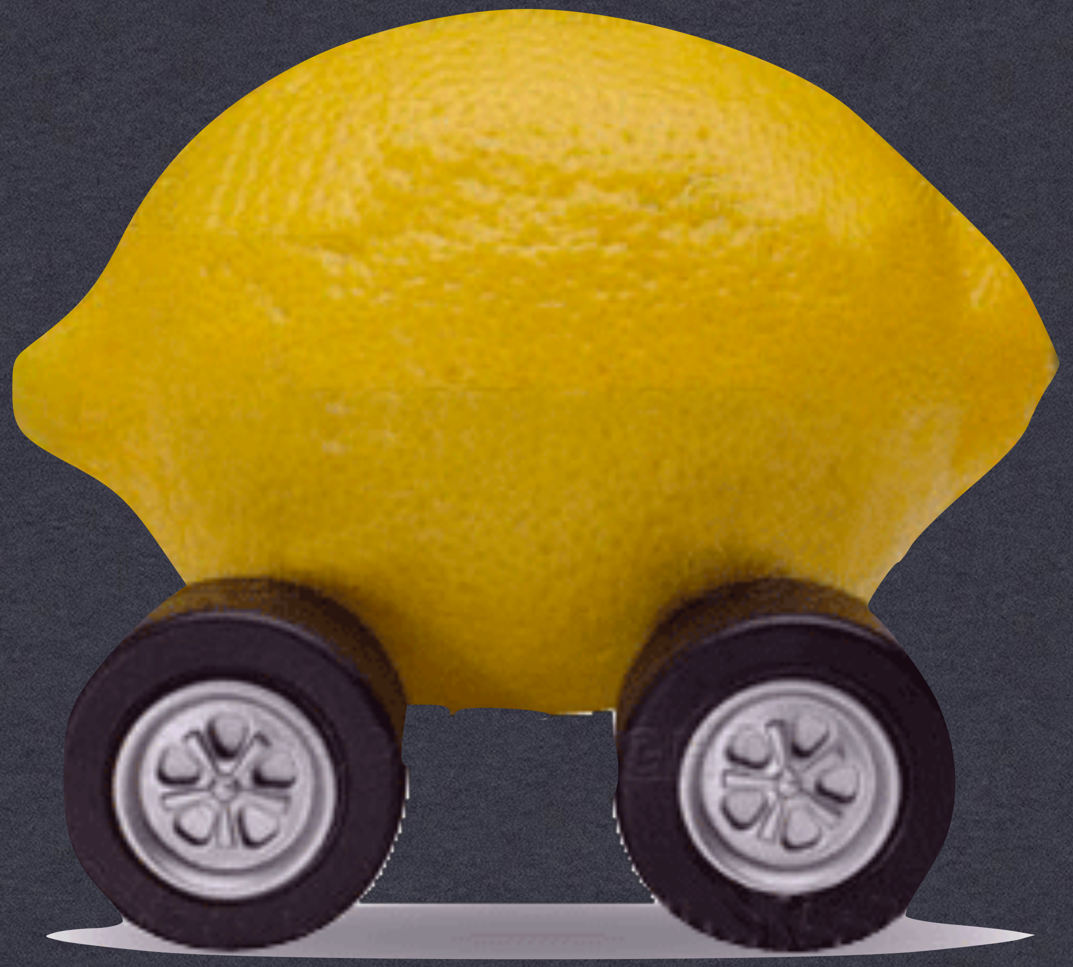
For Sale
(Customer View)

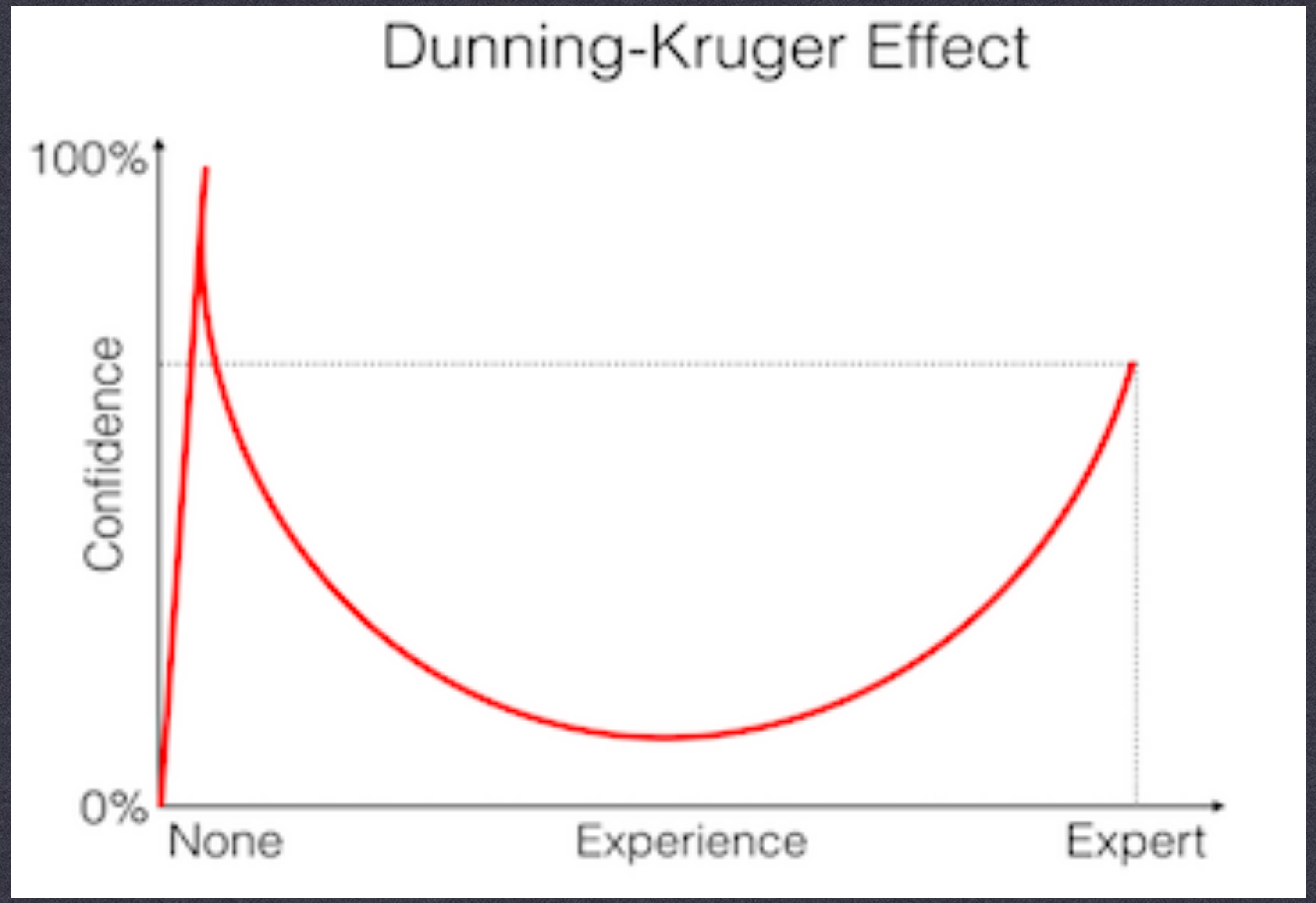


For Sale

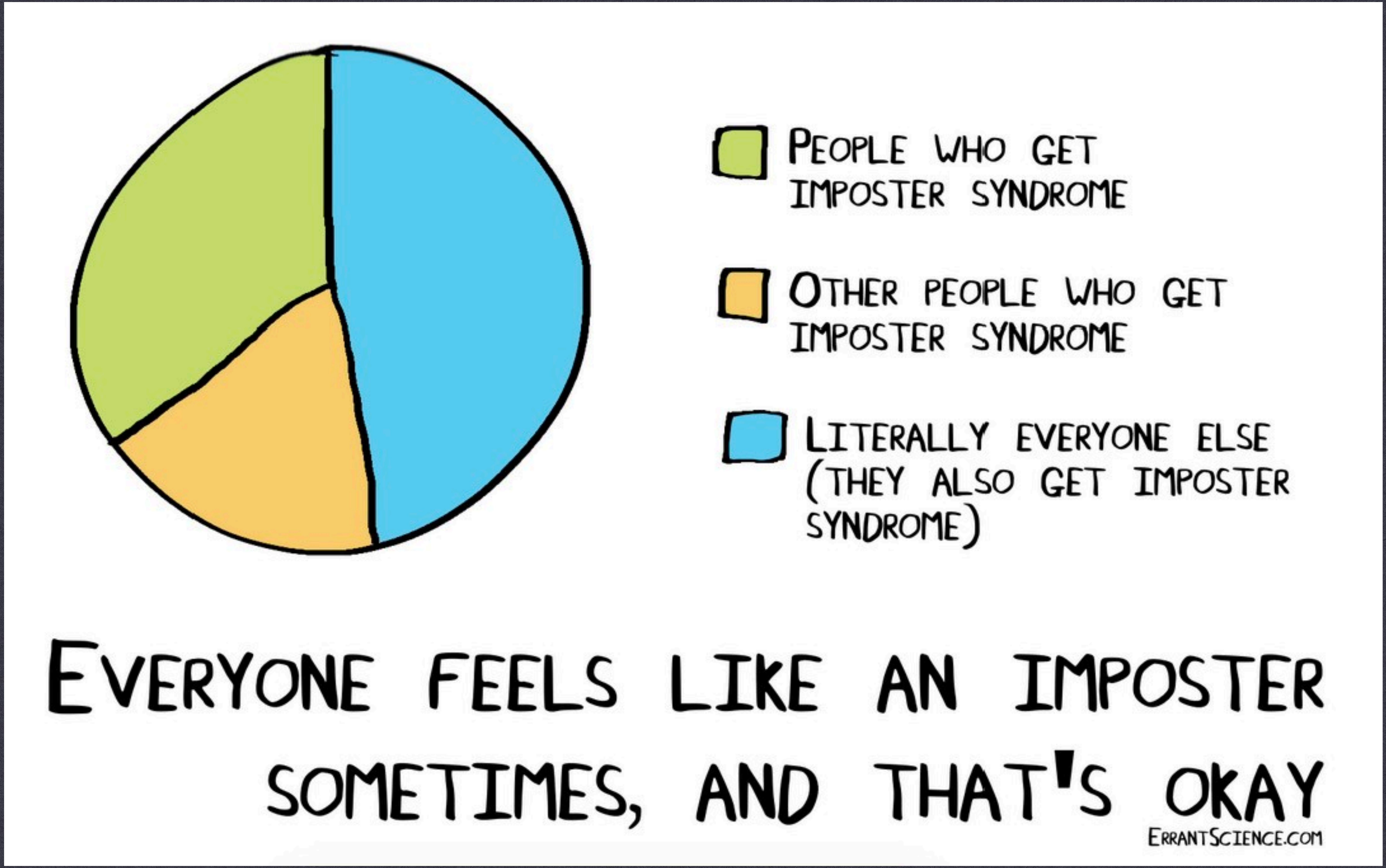

For Sale

For Sale




Dunning-Kruger Effect
100%
0%
Confidence
None
Experience
Expert

All these people really seem to have it together, and I still have no idea what's going on.
azilliondollarscomics.com


🟩 People who get imposter syndrome
🟨 Other people who get imposter syndrome
🟦 Literally everyone else (they also get imposter syndrome)

Everyone feels like an imposter sometimes, and that's okay

ErrantScience.com

Well Discussed

Possibly Misguided

thinkst

Now, how did I come to do this study?

...

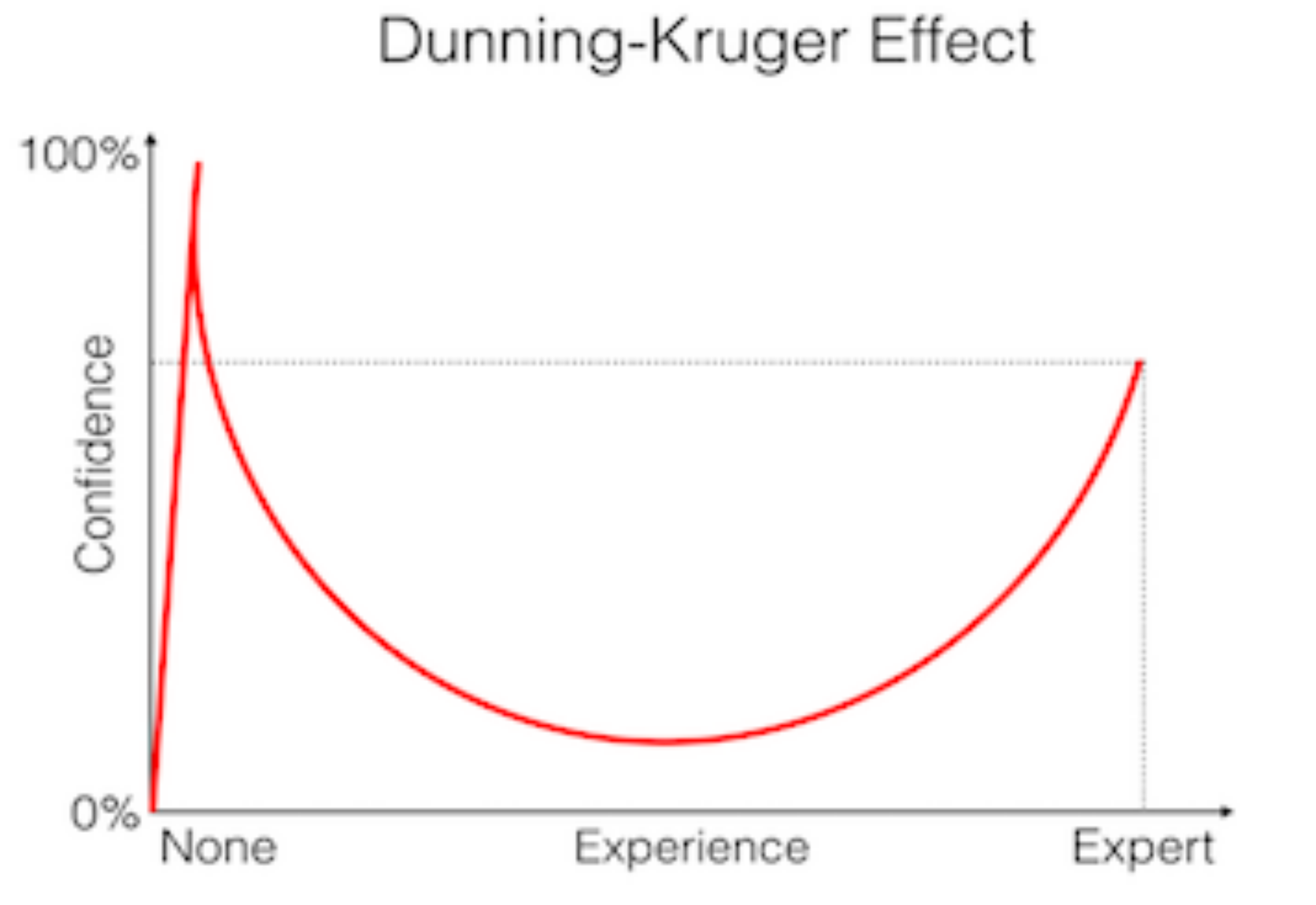
I saw I was a stooge.

I saw Feynman up close.
I saw Fermi and Teller.
I saw Oppenheimer.
I saw Hans Bethe..

Why this talk?

OLD MAN YELLS AT CLOUD

DANGER



Dunning-Kruger Effect

More people than ever..

More money than ever..

More hacks than ever..

Hypothesis

We are currently sucking

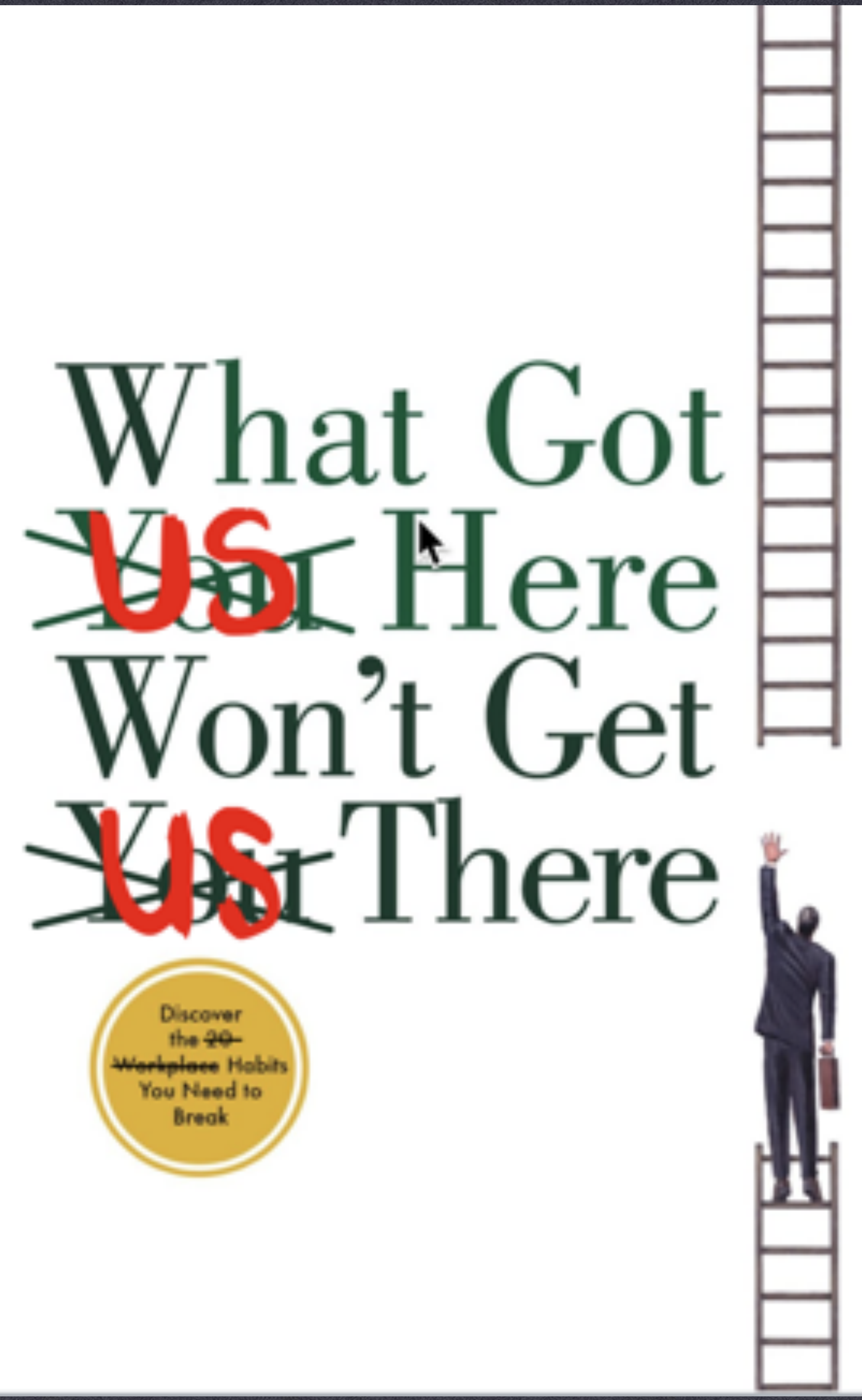
…and we are sucking because while we think everyone else is sucking,

we think we are doing just fine…

the hard thing

(about the hard things)

thinkst
applied research

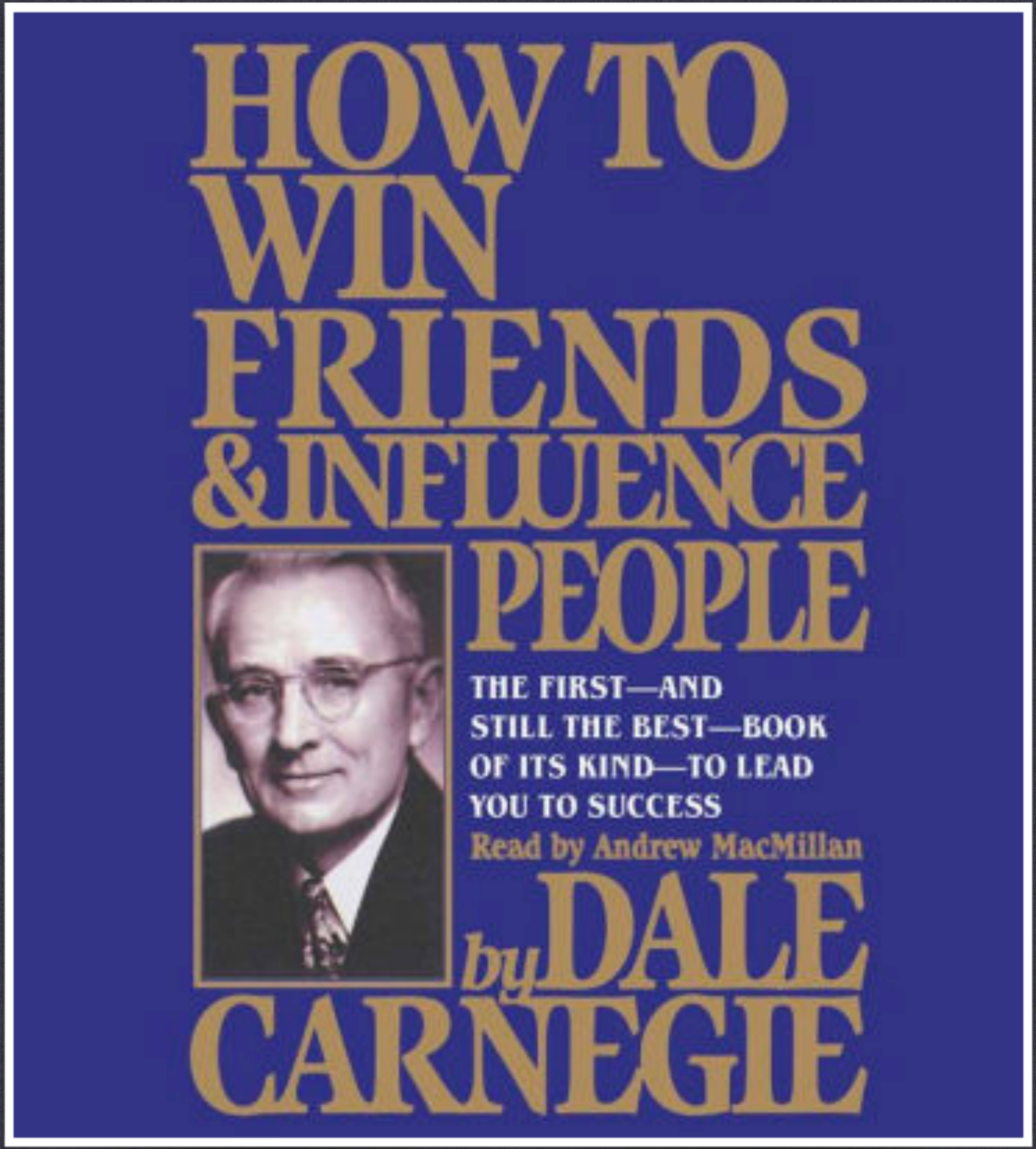


What Got ~~You~~ us Here Won't Get ~~You~~ us There

Discover the ~~20~~ ~~Workplace~~ Habits You Need to Break

@haroonmeer
Thinkst

Our personality defects



HOW TO WIN FRIENDS & INFLUENCE PEOPLE

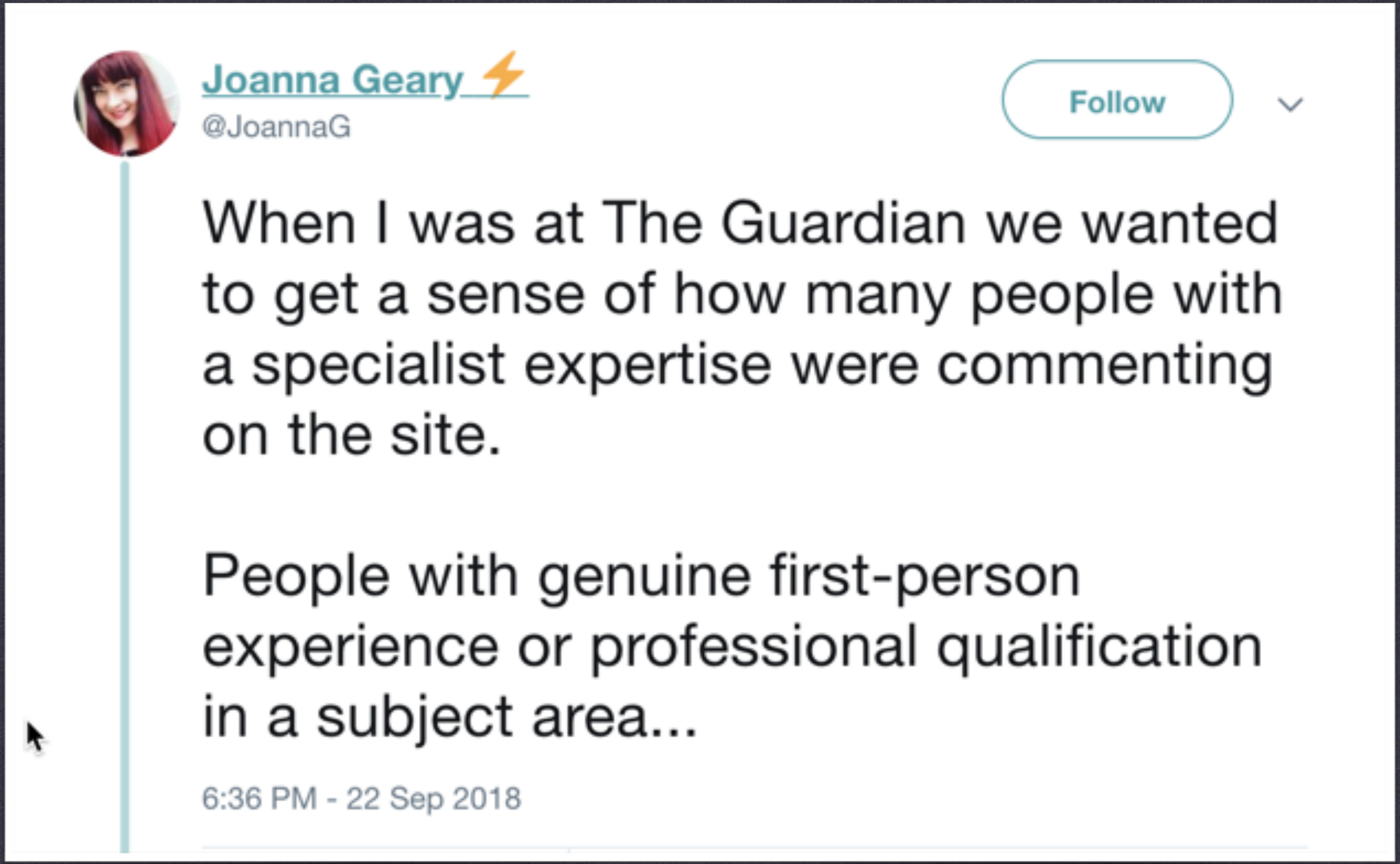
THE FIRST—AND STILL THE BEST—BOOK OF ITS KIND—TO LEAD YOU TO SUCCESS

Read by Andrew MacMillan

by DALE CARNEGIE

Give it 5 minutes..

https://signalvnoise.com/posts/3124-give-it-five-minutes



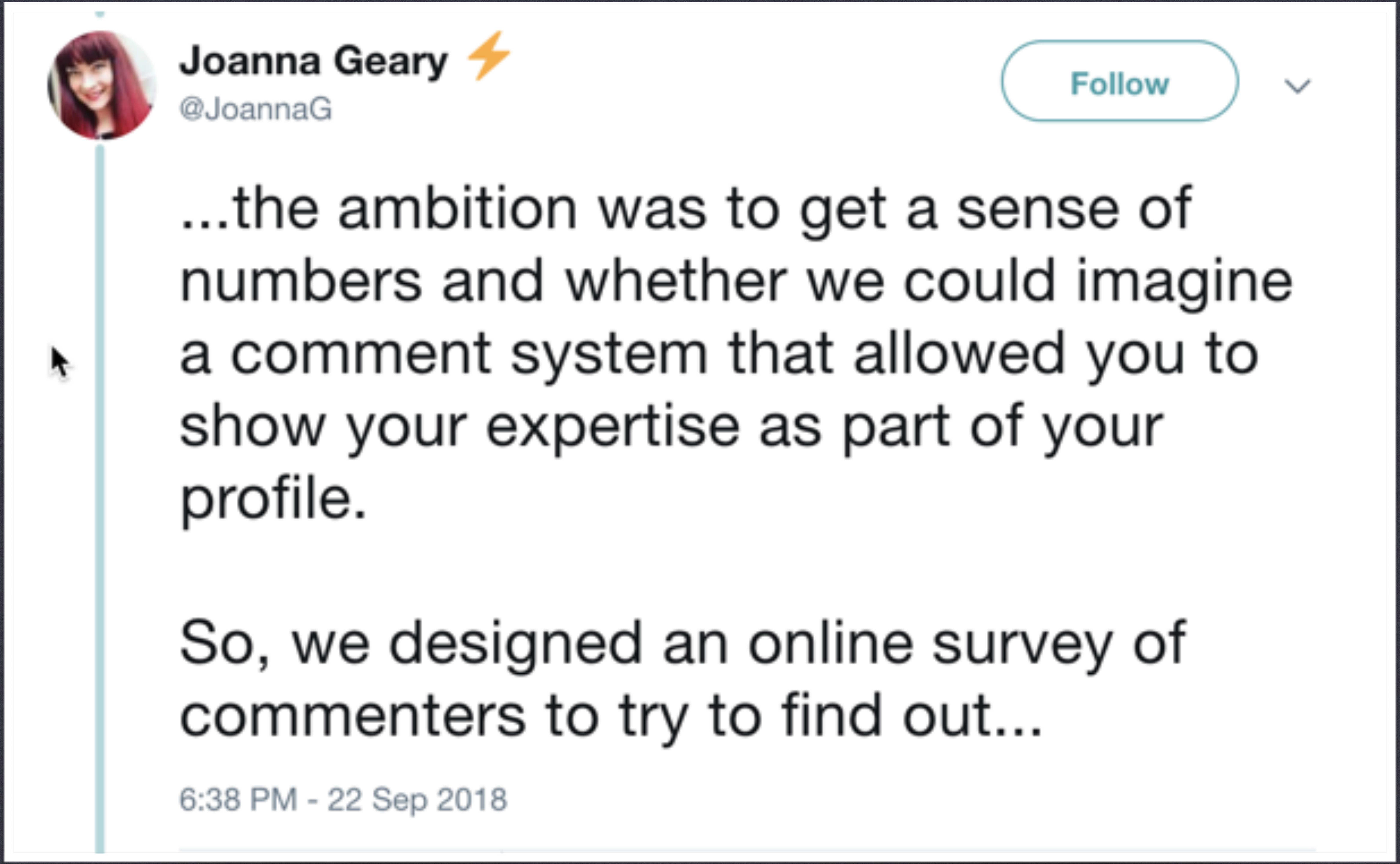
Joanna Geary ⚡
@JoannaG

When I was at The Guardian we wanted to get a sense of how many people with a specialist expertise were commenting on the site.

People with genuine first-person experience or professional qualification in a subject area...

6:36 PM - 22 Sep 2018

https://twitter.com/joannag/status/1043539467339030528?s=21



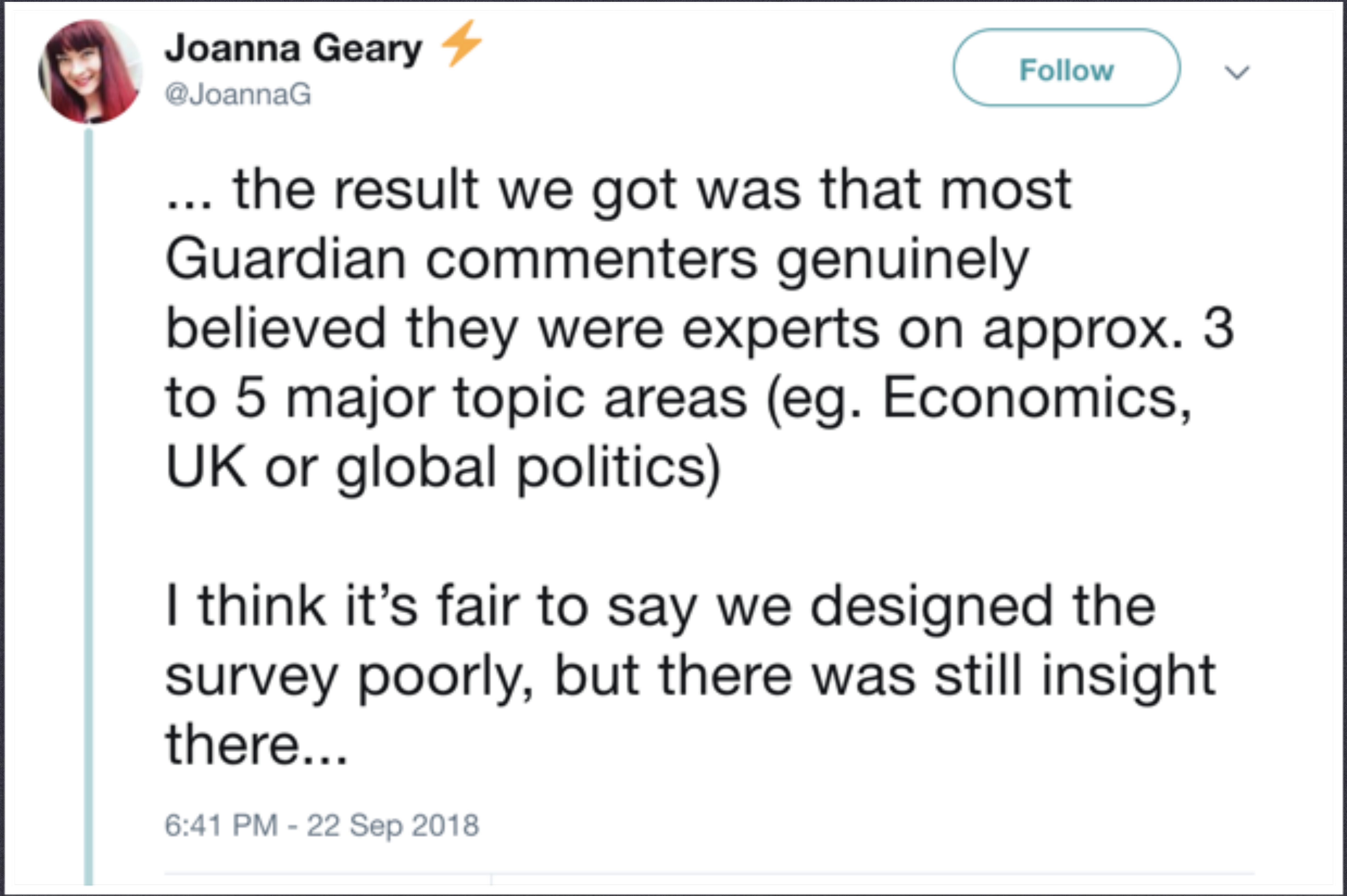
Joanna Geary ⚡
@JoannaG

...the ambition was to get a sense of numbers and whether we could imagine a comment system that allowed you to show your expertise as part of your profile.

So, we designed an online survey of commenters to try to find out...

6:38 PM - 22 Sep 2018

https://twitter.com/joannag/status/1043539467339030528?s=21



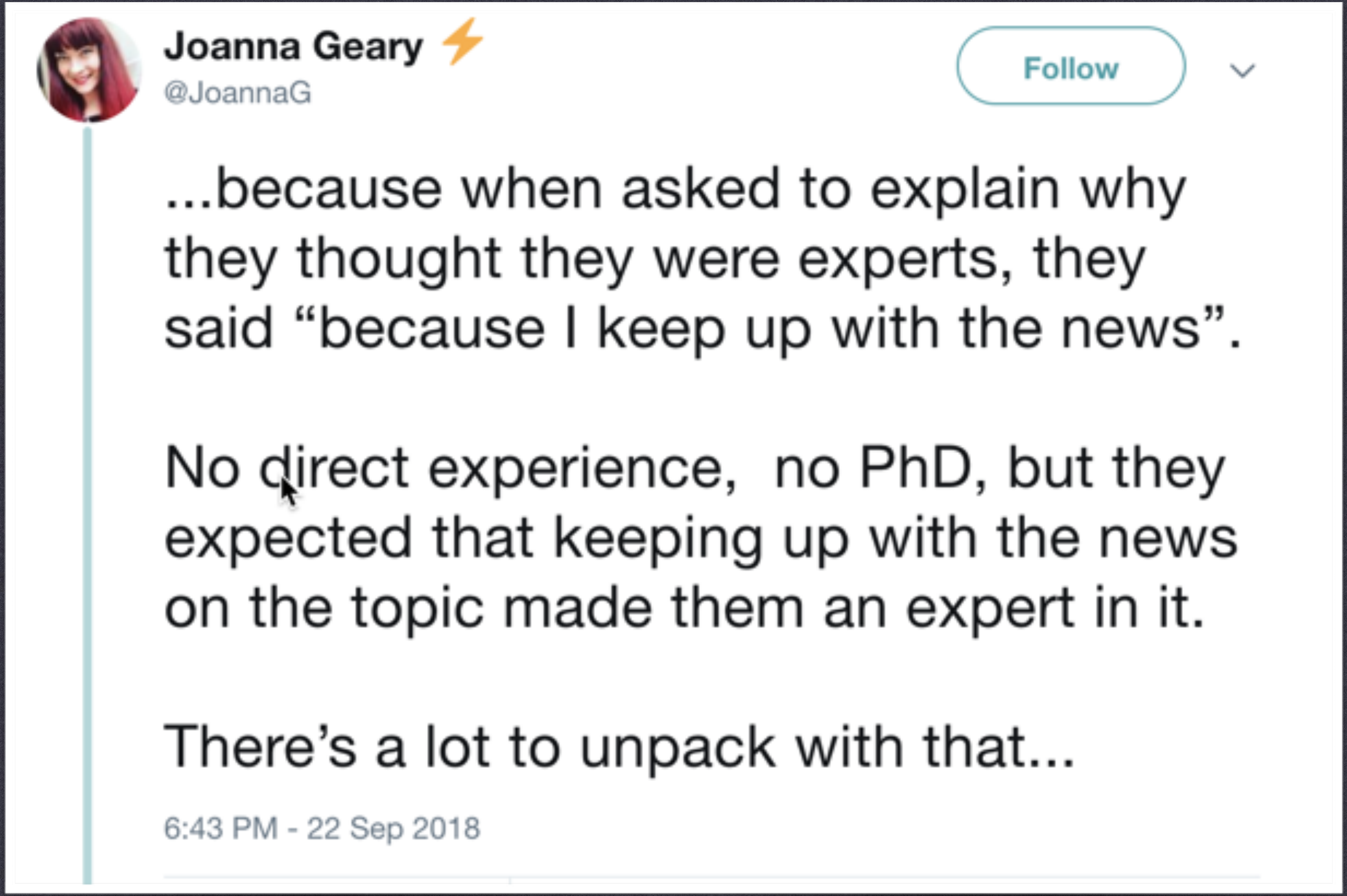
Joanna Geary ⚡
@JoannaG

... the result we got was that most Guardian commenters genuinely believed they were experts on approx. 3 to 5 major topic areas (eg. Economics, UK or global politics)

I think it's fair to say we designed the survey poorly, but there was still insight there...

6:41 PM - 22 Sep 2018

https://twitter.com/joannag/status/1043539467339030528?s=21



Joanna Geary ⚡
@JoannaG

...because when asked to explain why they thought they were experts, they said “because I keep up with the news”.

No direct experience, no PhD, but they expected that keeping up with the news on the topic made them an expert in it.

There’s a lot to unpack with that...

6:43 PM - 22 Sep 2018

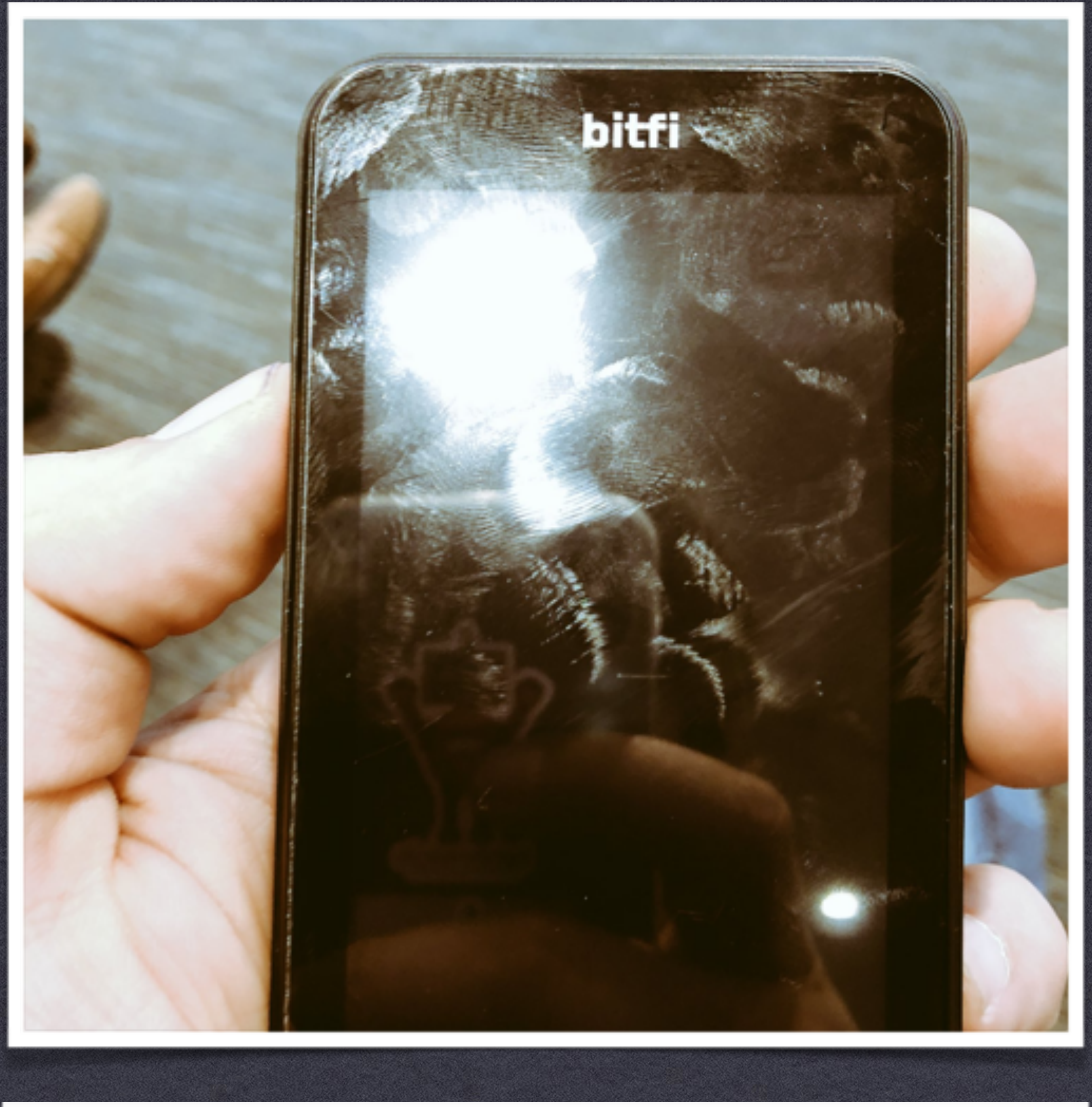
https://twitter.com/joannag/status/1043539467339030528?s=21

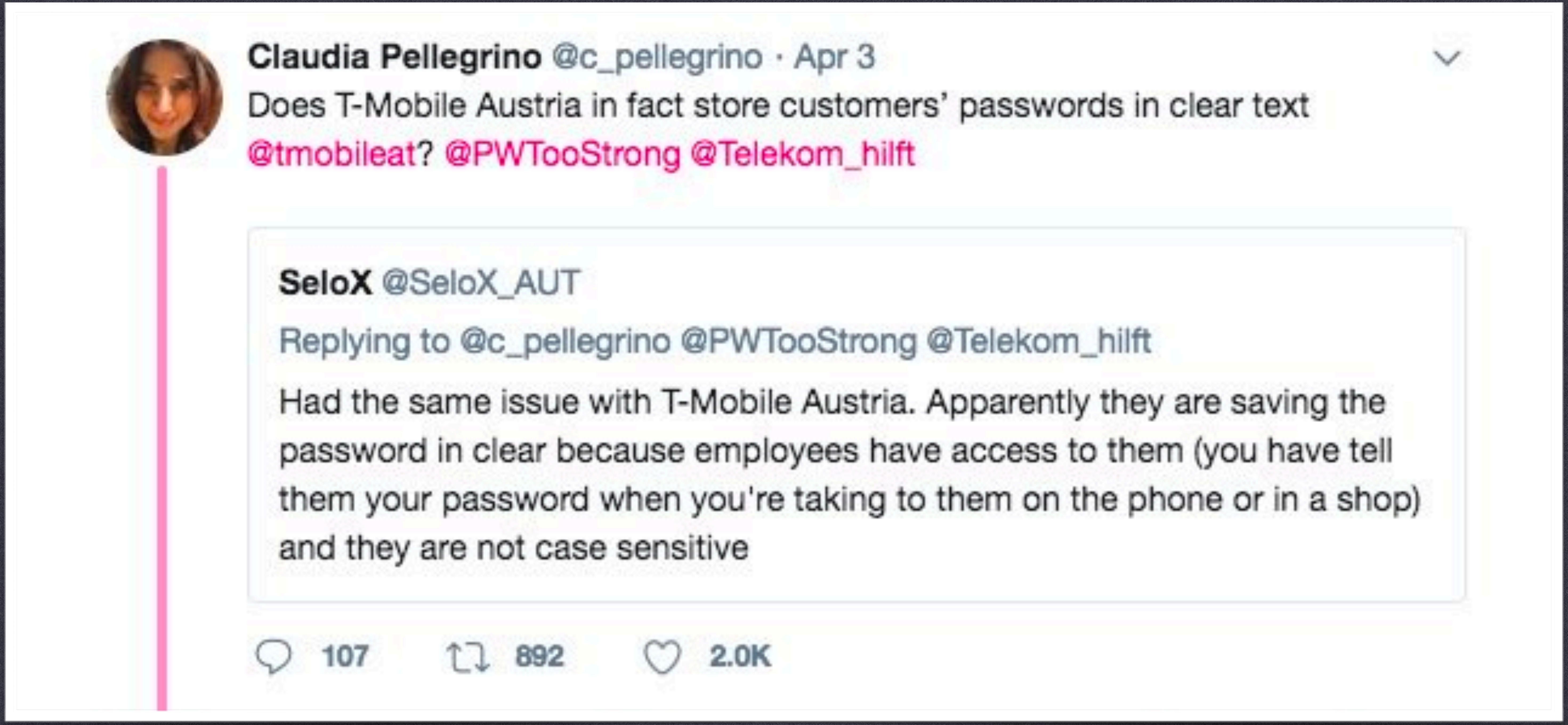
🙄

following the News doesn’t make you an expert..

bitfi
bitfi

“This bounty program is not intended to help **Bitfi** to identify **security** vulnerabilities since we already claim that **our security is absolute**”

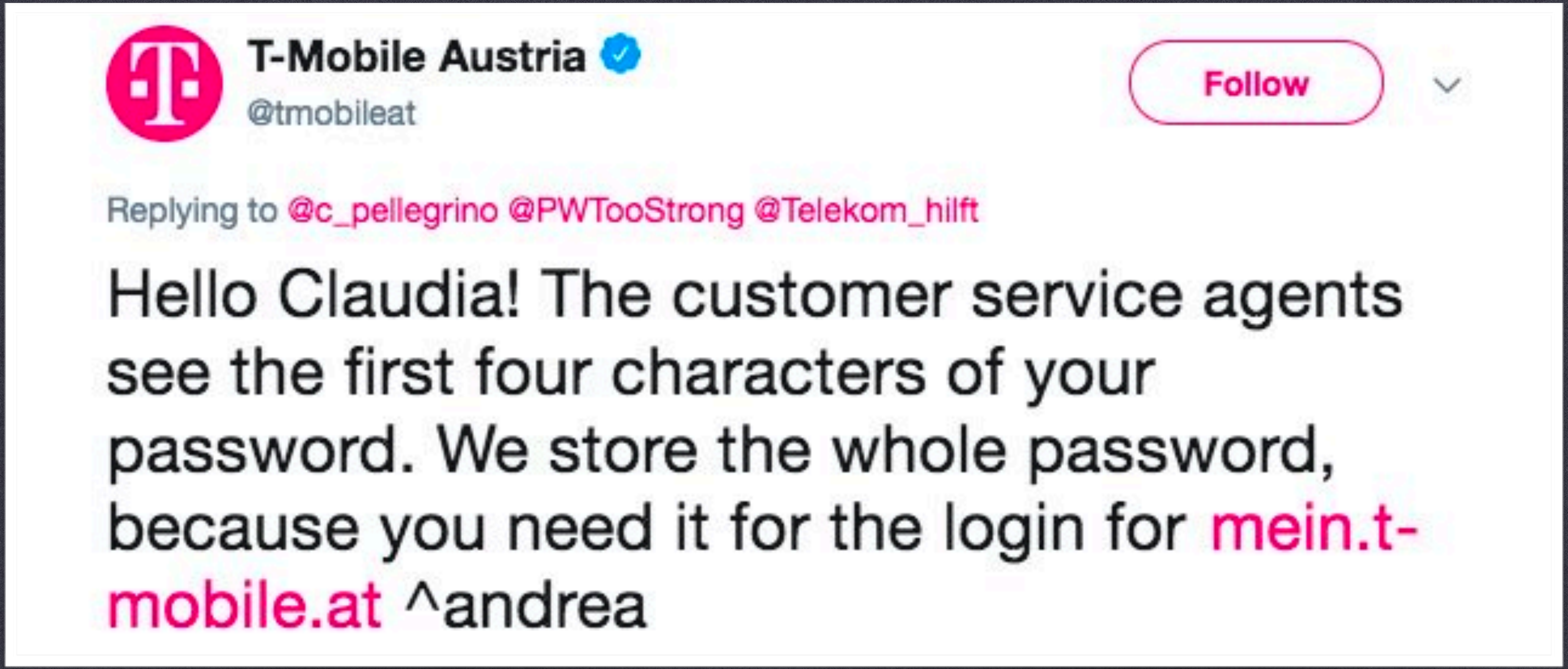




Claudia Pellegrino @c_pellegrino · Apr 3

Does T-Mobile Austria in fact store customers' passwords in clear text @tmobileat? @PWTooStrong @Telekom_hilft

> **SeloX** @SeloX_AUT
>
> Replying to @c_pellegrino @PWTooStrong @Telekom_hilft
>
> Had the same issue with T-Mobile Austria. Apparently they are saving the password in clear because employees have access to them (you have tell them your password when you're taking to them on the phone or in a shop) and they are not case sensitive

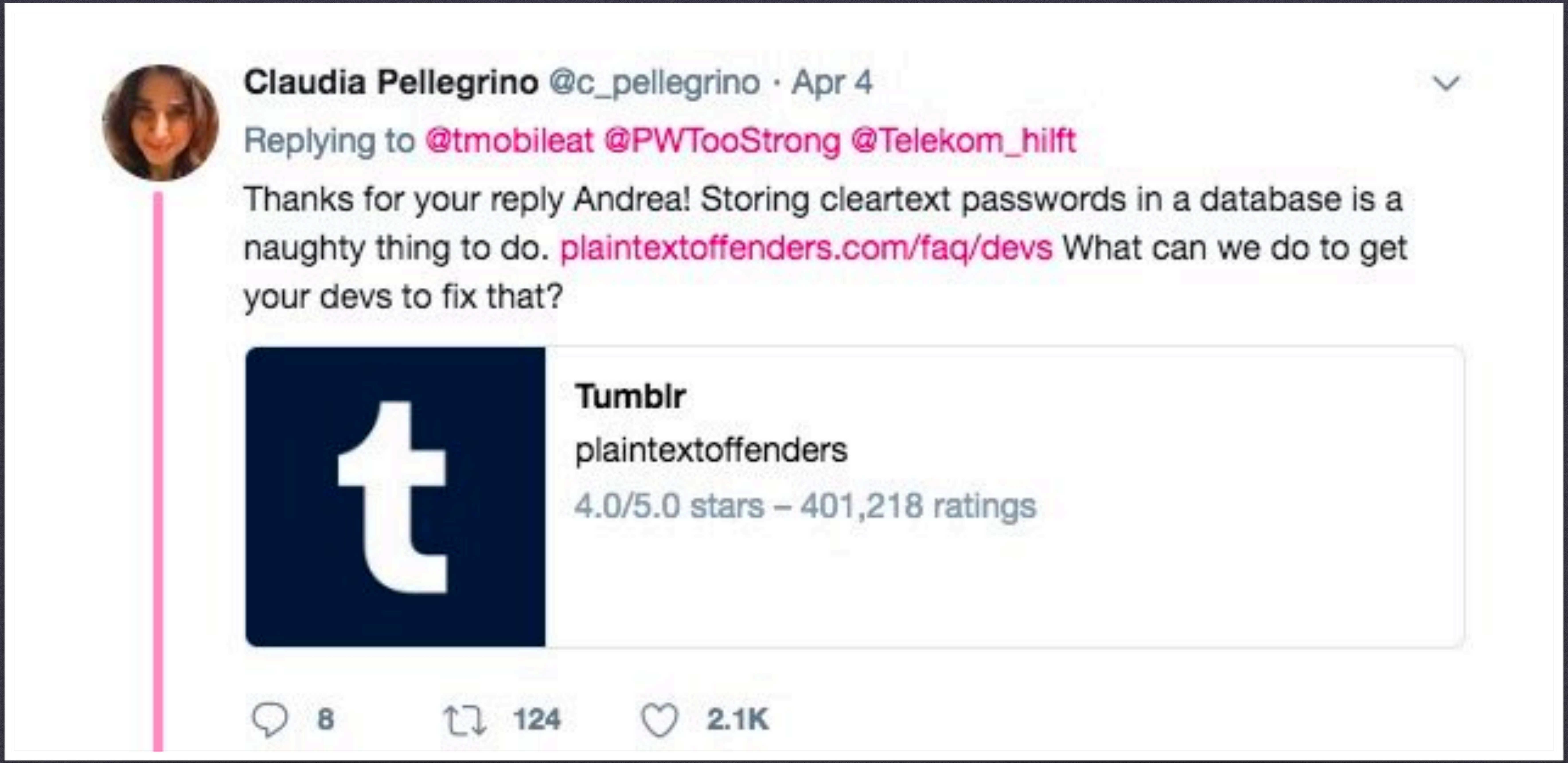


T-Mobile Austria

@tmobileat

Replying to @c_pellegrino @PWTooStrong @Telekom_hilft

Hello Claudia! The customer service agents see the first four characters of your password. We store the whole password, because you need it for the login for mein.t-mobile.at ^andrea



Claudia Pellegrino @c_pellegrino · Apr 4

Replying to @tmobileat @PWTooStrong @Telekom_hilft

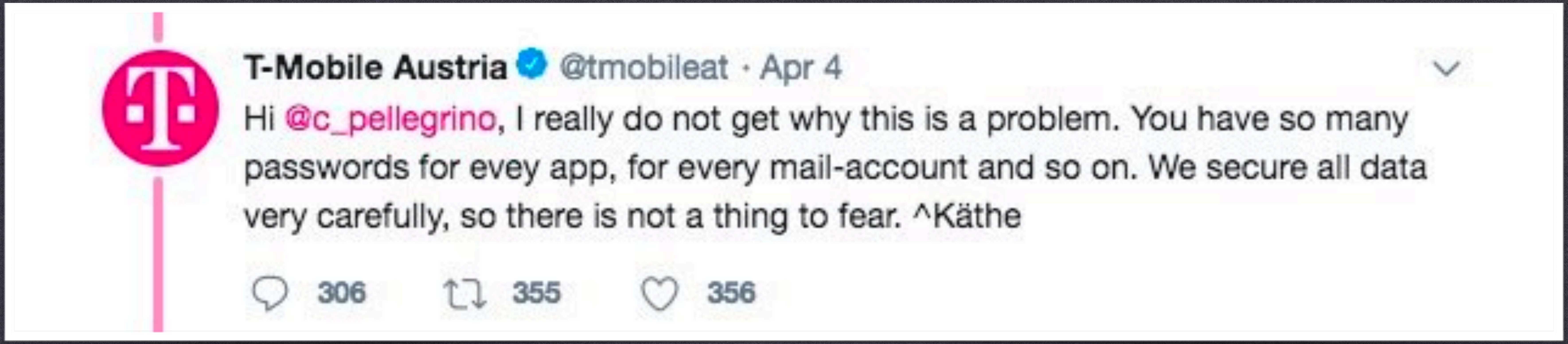
Thanks for your reply Andrea! Storing cleartext passwords in a database is a naughty thing to do. plaintextoffenders.com/faq/devs What can we do to get your devs to fix that?

Tumblr

plaintextoffenders

4.0/5.0 stars – 401,218 ratings

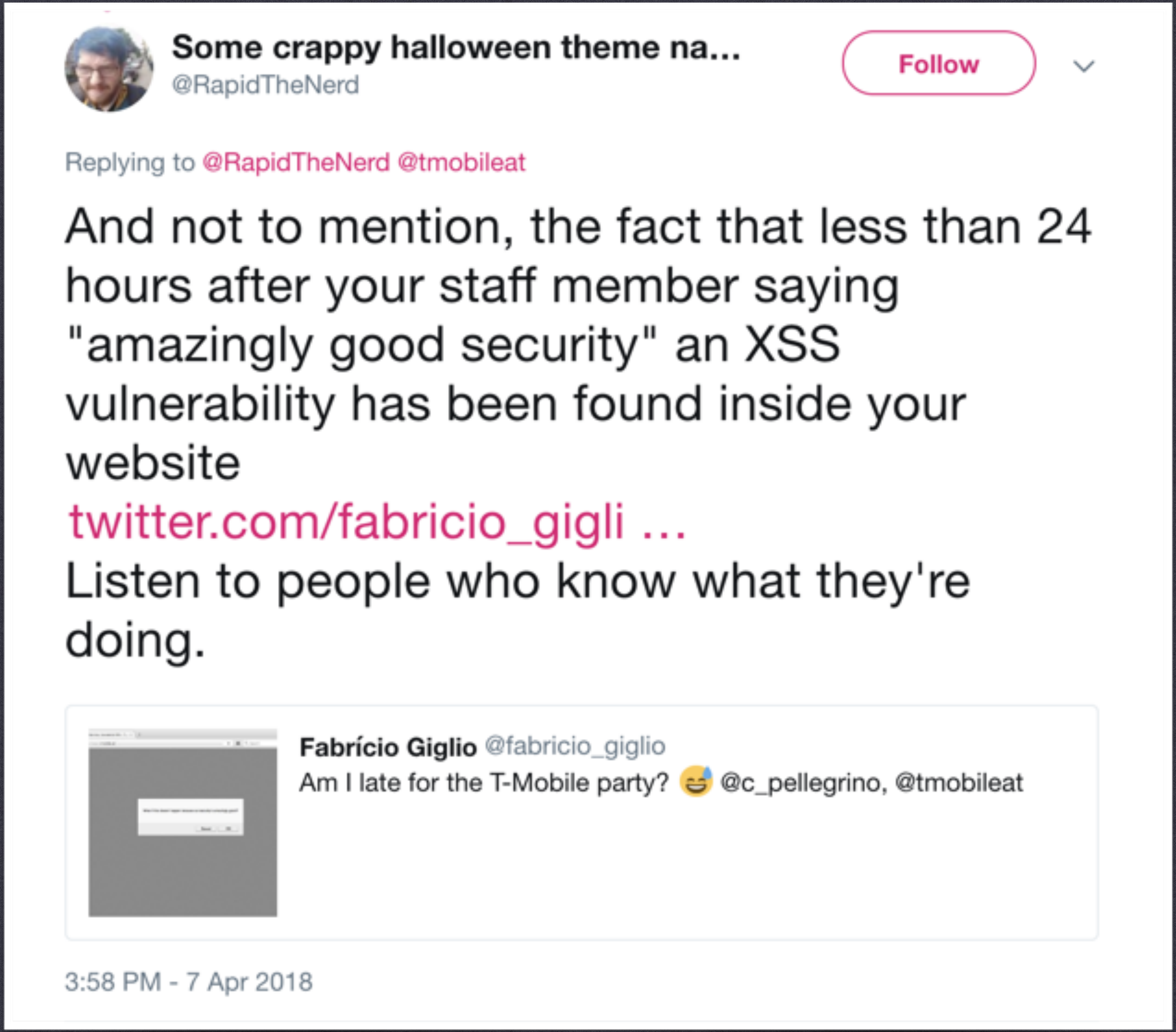
8 124 2.1K



T-Mobile Austria @tmobileat · Apr 4

Hi @c_pellegrino, I really do not get why this is a problem. You have so many passwords for evey app, for every mail-account and so on. We secure all data very carefully, so there is not a thing to fear. ^Käthe

306 355 356



Some crappy halloween theme na...
@RapidTheNerd

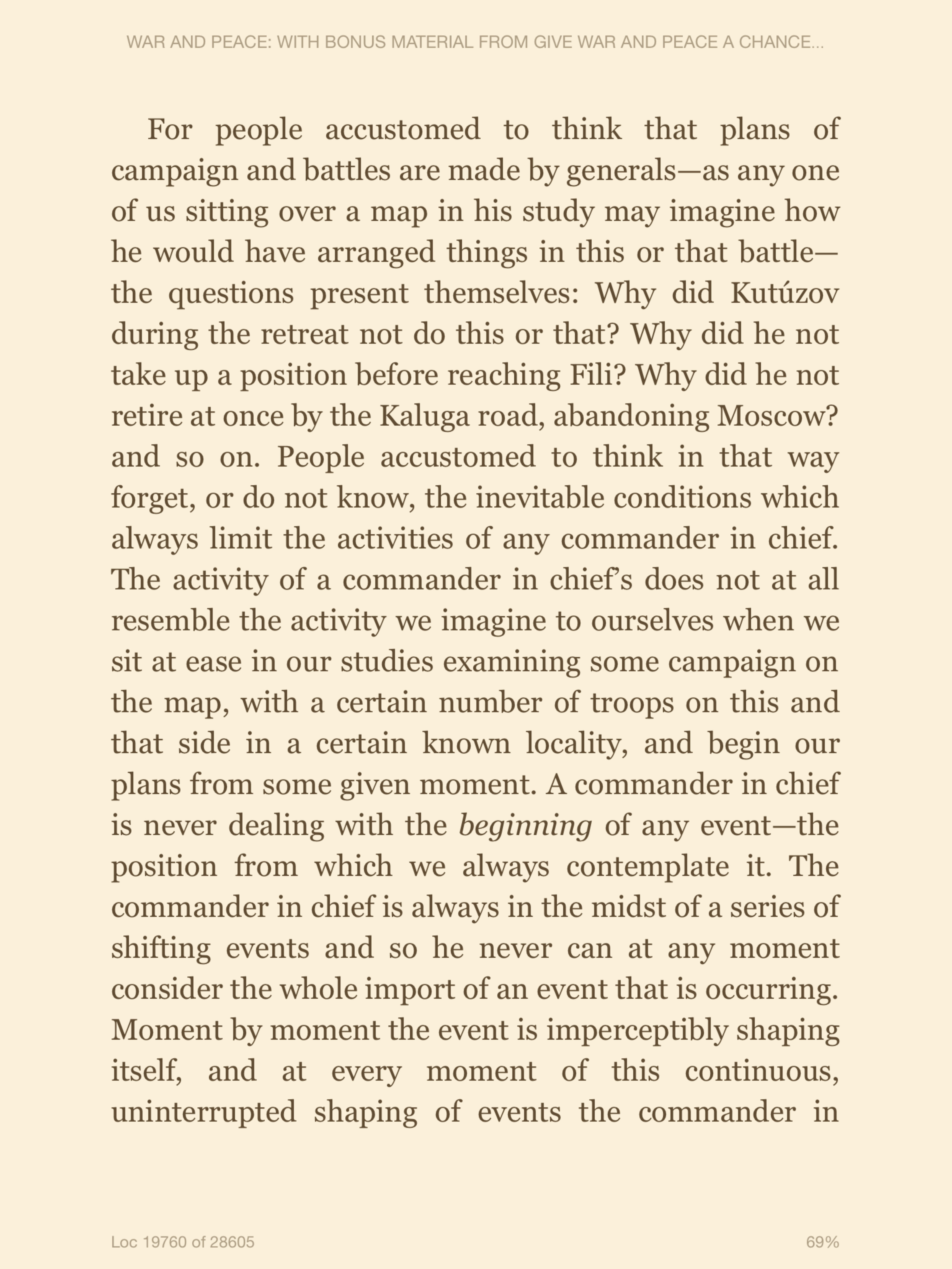
Replying to @RapidTheNerd @tmobileat

And not to mention, the fact that less than 24 hours after your staff member saying "amazingly good security" an XSS vulnerability has been found inside your website
twitter.com/fabricio_gigli ...
Listen to people who know what they're doing.

Fabrício Giglio @fabricio_giglio
Am I late for the T-Mobile party? 😅 @c_pellegrino, @tmobileat

3:58 PM - 7 Apr 2018

“Why didn’t they just do XX?”



WAR AND PEACE: WITH BONUS MATERIAL FROM GIVE WAR AND PEACE A CHANCE...

For people accustomed to think that plans of campaign and battles are made by generals—as any one of us sitting over a map in his study may imagine how he would have arranged things in this or that battle—the questions present themselves: Why did Kutúzov during the retreat not do this or that? Why did he not take up a position before reaching Fili? Why did he not retire at once by the Kaluga road, abandoning Moscow? and so on. People accustomed to think in that way forget, or do not know, the inevitable conditions which always limit the activities of any commander in chief. The activity of a commander in chief's does not at all resemble the activity we imagine to ourselves when we sit at ease in our studies examining some campaign on the map, with a certain number of troops on this and that side in a certain known locality, and begin our plans from some given moment. A commander in chief is never dealing with the *beginning* of any event—the position from which we always contemplate it. The commander in chief is always in the midst of a series of shifting events and so he never can at any moment consider the whole import of an event that is occurring. Moment by moment the event is imperceptibly shaping itself, and at every moment of this continuous, uninterrupted shaping of events the commander in

Loc 19760 of 28605

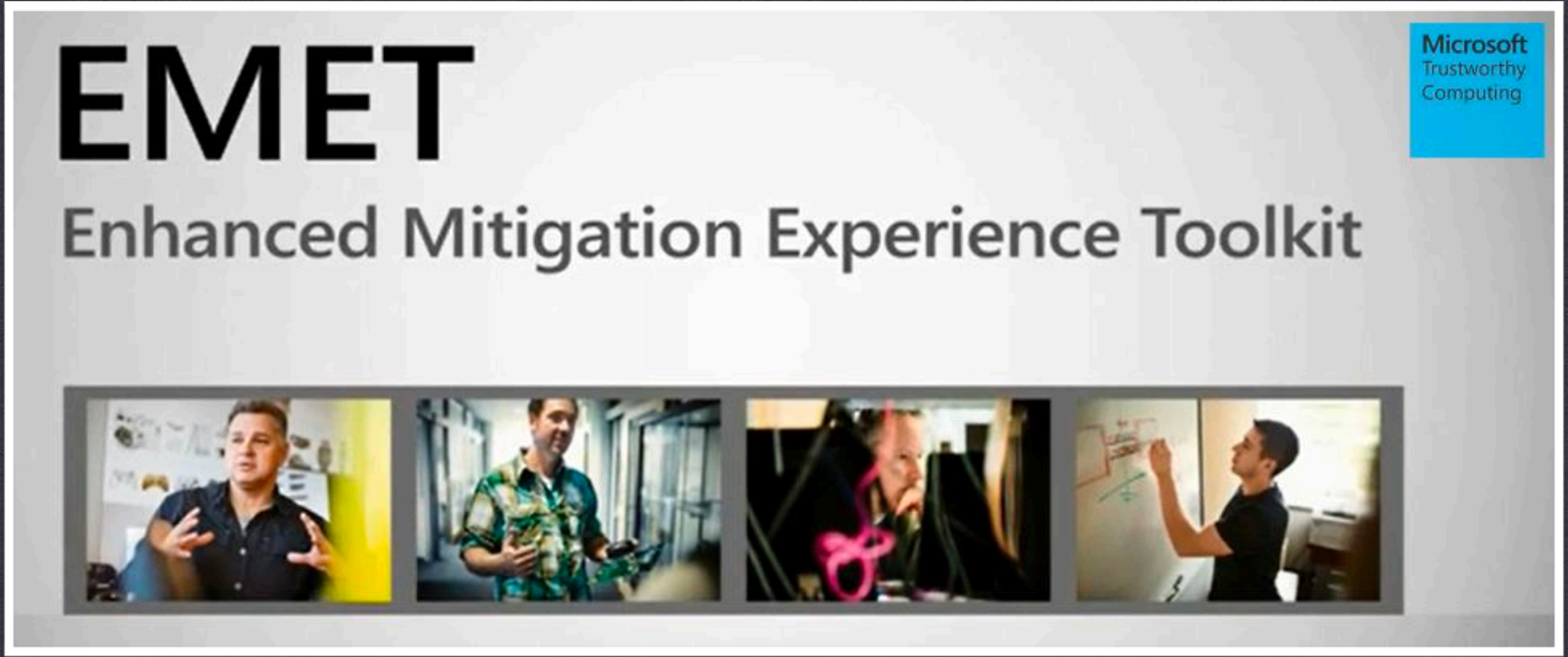
69%

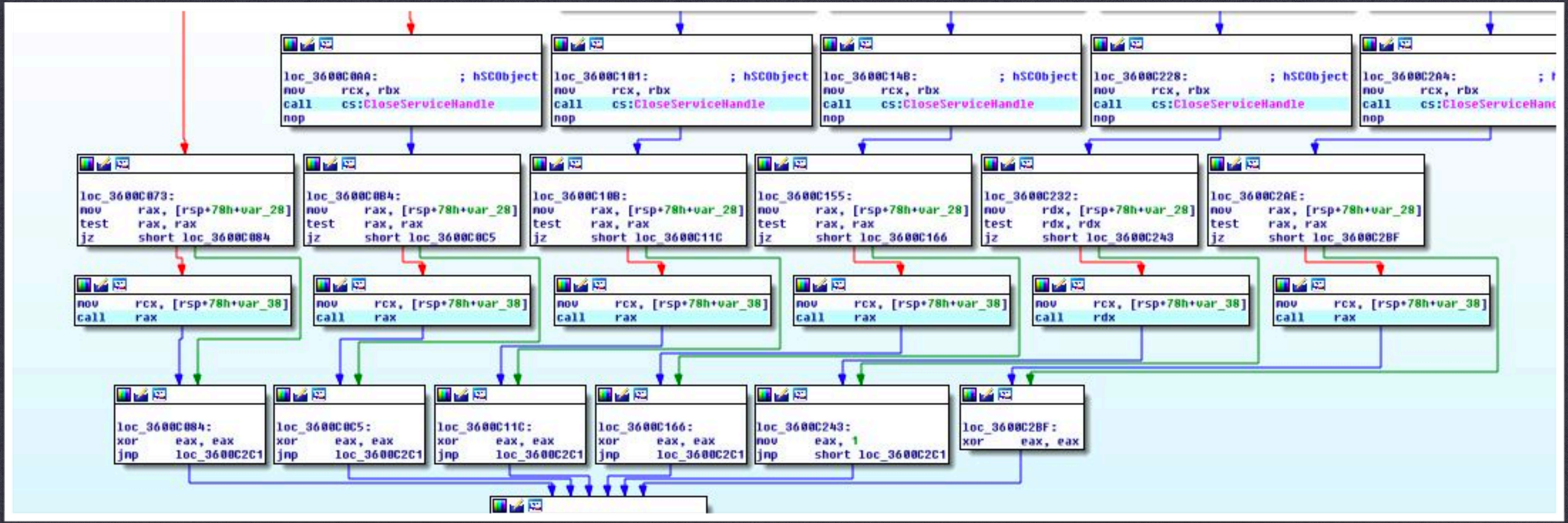
For people accustomed to think that plans of campaign and battles are made by generals- as any one of us sitting over a map in his study may imagine how he would have arranged things in this or that battle- the questions present themselves: Why did Kutuzov during the retreat not do this or that? Why did he not take up a position before reaching Fili? Why did he not retire at once by the Kaluga road, abandoning Moscow? and so on. People accustomed to think in that way forget, or do not know, the inevitable conditions which always limit the activities of any commander in chief. The activity of a commander in chief does not all resemble the activity we imagine to ourselves when we sit at case in our studies examining some campaign on the map, with a certain number of troops on this and that side in a certain known locality, and begin our plans from some given moment. **A commander in chief is never dealing with the beginning of any event- the position from which we always contemplate it. The commander in chief is always in the midst of a series of shifting events and so he never can at any moment consider the whole import of an event that is occurring.** Moment by moment the event is imperceptibly shaping itself, and at every moment of this continuous, uninterrupted shaping of events the commander in chief is in the midst of a most complex play of intrigues, worries, contingencies, authorities, projects, counsels, threats, and deceptions and is continually obliged to reply to innumerable questions addressed to him, which constantly conflict with one another.

War and Peace by Leo Tolstoy

Discussions post-breach are easy

Choosing is the hard part





```
loc_3600C0AA:           ; hSCObject
mov     rcx, rbx
call    cs:CloseServiceHandle
nop
```

```
loc_3600C101:           ; hSCObject
mov     rcx, rbx
call    cs:CloseServiceHandle
nop
```

```
loc_3600C14B:           ; hSCObject
mov     rcx, rbx
call    cs:CloseServiceHandle
nop
```

```
loc_3600C228:           ; hSCObject
mov     rcx, rbx
call    cs:CloseServiceHandle
nop
```

```
loc_3600C2A4:           ; h
mov     rcx, rbx
call    cs:CloseServiceHanc
nop
```

```
loc_3600C073:
mov     rax, [rsp+78h+var_28]
test    rax, rax
jz      short loc_3600C084
```

```
loc_3600C0B4:
mov     rax, [rsp+78h+var_28]
test    rax, rax
jz      short loc_3600C0C5
```

```
loc_3600C10B:
mov     rax, [rsp+78h+var_28]
test    rax, rax
jz      short loc_3600C11C
```

```
loc_3600C155:
mov     rax, [rsp+78h+var_28]
test    rax, rax
jz      short loc_3600C166
```

```
loc_3600C232:
mov     rdx, [rsp+78h+var_28]
test    rdx, rdx
jz      short loc_3600C243
```

```
loc_3600C2AE:
mov     rax, [rsp+78h+var_28]
test    rax, rax
jz      short loc_3600C2BF
```

```
mov     rcx, [rsp+78h+var_38]
call    rax
```

```
mov     rcx, [rsp+78h+var_38]
call    rax
```

```
mov     rcx, [rsp+78h+var_38]
call    rax
```

```
mov     rcx, [rsp+78h+var_38]
call    rax
```

```
mov     rcx, [rsp+78h+var_38]
call    rdx
```

```
mov     rcx, [rsp+78h+var_38]
call    rax
```

```
loc_3600C084:
xor     eax, eax
jmp     loc_3600C2C1
```

```
loc_3600C0C5:
xor     eax, eax
jmp     loc_3600C2C1
```

```
loc_3600C11C:
xor     eax, eax
jmp     loc_3600C2C1
```

```
loc_3600C166:
xor     eax, eax
jmp     loc_3600C2C1
```

```
loc_3600C243:
mov     eax, 1
jmp     short loc_3600C2C1
```

```
loc_3600C2BF:
xor     eax, eax
```

Community Chest

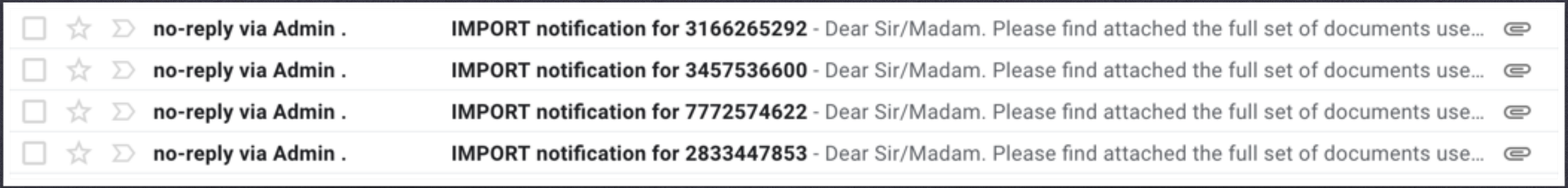
GET OUT
OF JAIL, FREE

THIS CARD MAY BE KEPT UNTIL NEEDED OR SOLD

© 1935 PARKER BROTHERS, INC.

In fact..

Learning from breaches is critical..

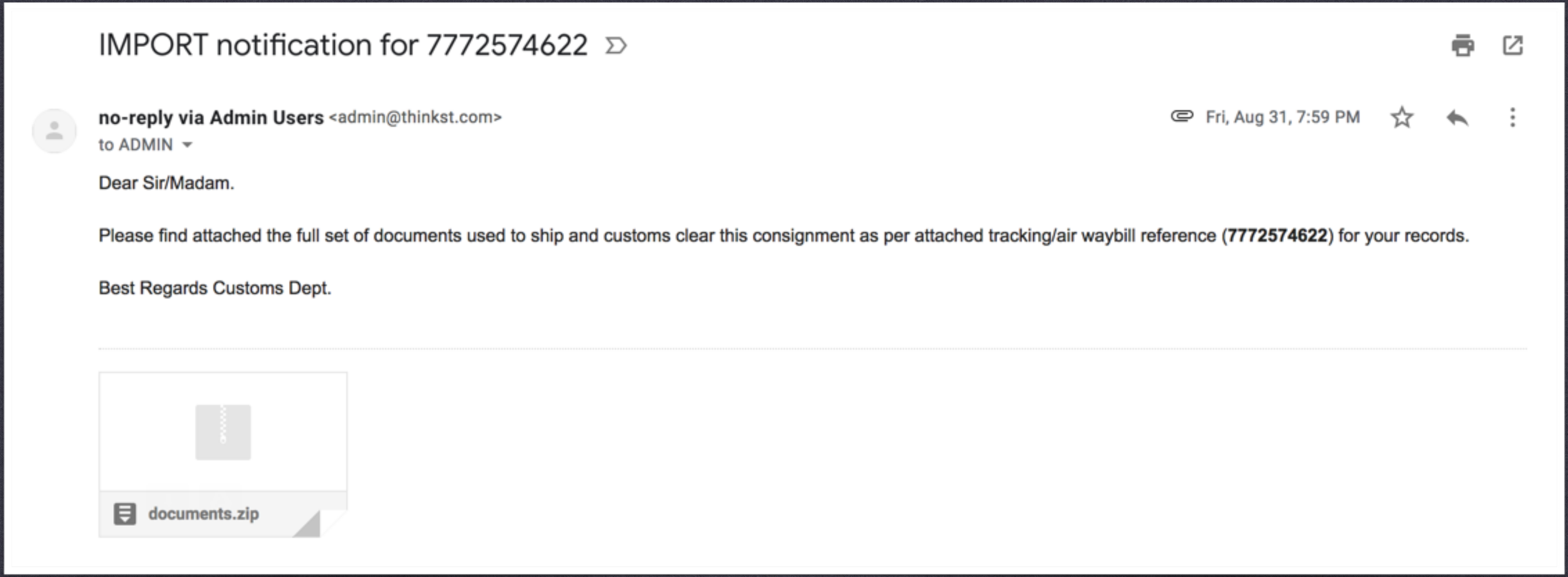


no-reply via Admin . **IMPORT notification for 3166265292** - Dear Sir/Madam. Please find attached the full set of documents use...

no-reply via Admin . **IMPORT notification for 3457536600** - Dear Sir/Madam. Please find attached the full set of documents use...

no-reply via Admin . **IMPORT notification for 7772574622** - Dear Sir/Madam. Please find attached the full set of documents use...

no-reply via Admin . **IMPORT notification for 2833447853** - Dear Sir/Madam. Please find attached the full set of documents use...



IMPORT notification for 7772574622

no-reply via Admin Users <admin@thinkst.com>
to ADMIN

Fri, Aug 31, 7:59 PM

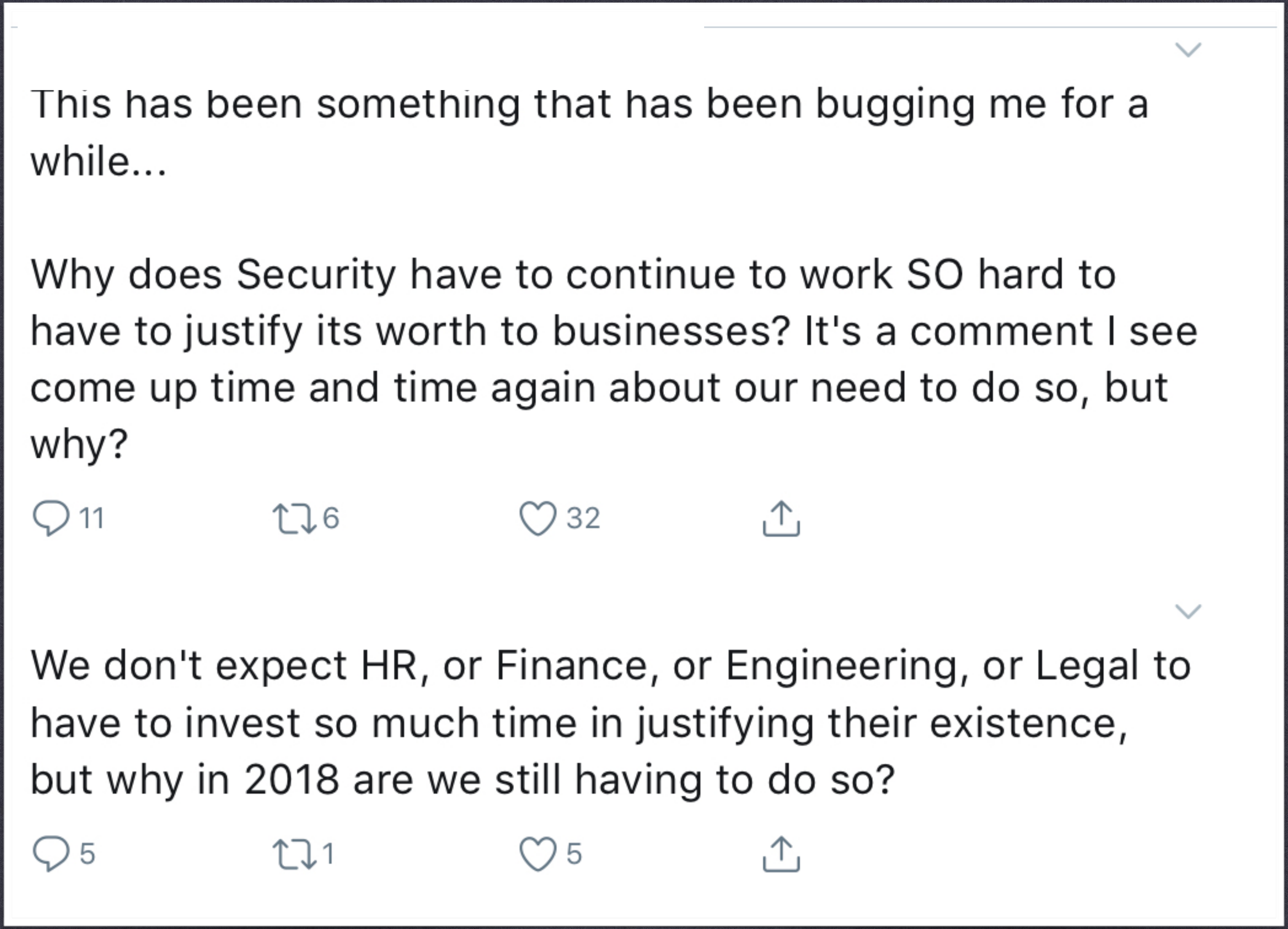
Dear Sir/Madam.

Please find attached the full set of documents used to ship and customs clear this consignment as per attached tracking/air waybill reference (**7772574622**) for your records.

Best Regards Customs Dept.

documents.zip

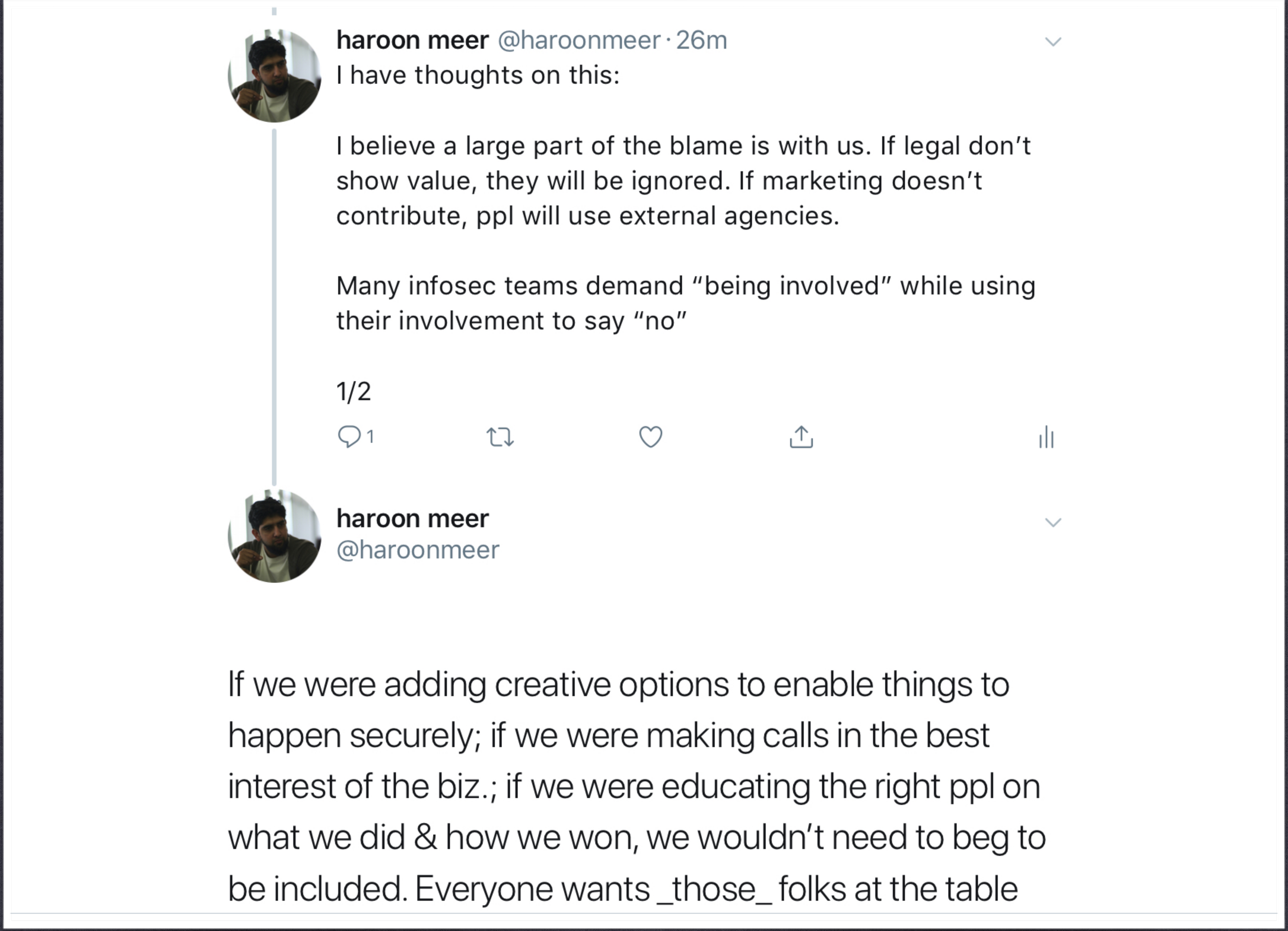
Blue-Teaming can be hard..



This has been something that has been bugging me for a while...

Why does Security have to continue to work SO hard to have to justify its worth to businesses? It's a comment I see come up time and time again about our need to do so, but why?

We don't expect HR, or Finance, or Engineering, or Legal to have to invest so much time in justifying their existence, but why in 2018 are we still having to do so?



I have thoughts on this:

I believe a large part of the blame is with us. If legal don’t show value, they will be ignored. If marketing doesn’t contribute, ppl will use external agencies.

Many infosec teams demand “being involved” while using their involvement to say “no”

1/2

If we were adding creative options to enable things to happen securely; if we were making calls in the best interest of the biz.; if we were educating the right ppl on what we did & how we won, we wouldn’t need to beg to be included. Everyone wants _those_ folks at the table

There are definite challenges

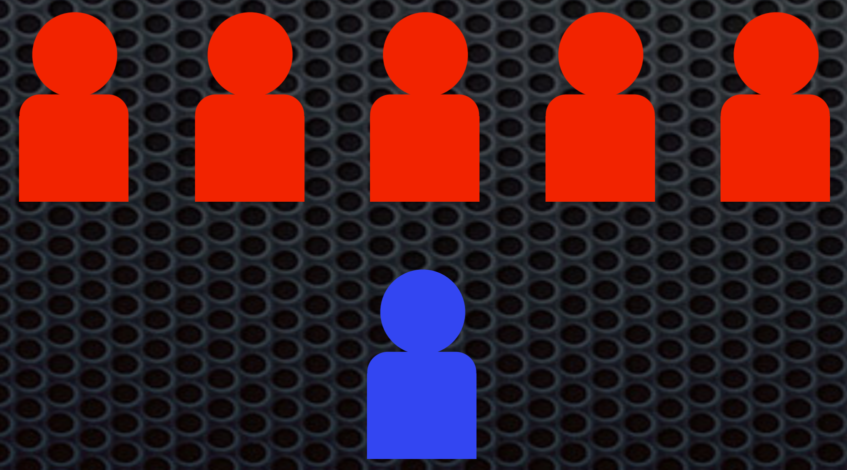
Learning the wrong lessons from Offense

@haroonmeer

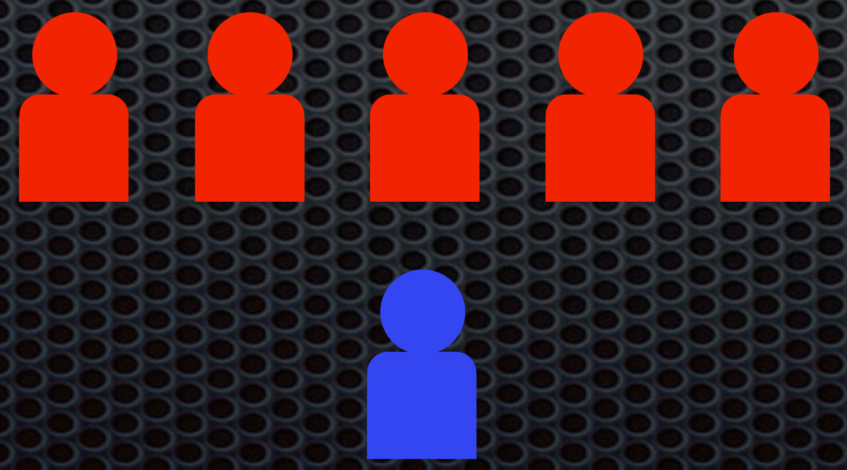
thinkst
applied research

https://t2.fi/2017/02/05/haroon-meer-keynote-2016/

Tight Feedback Loops



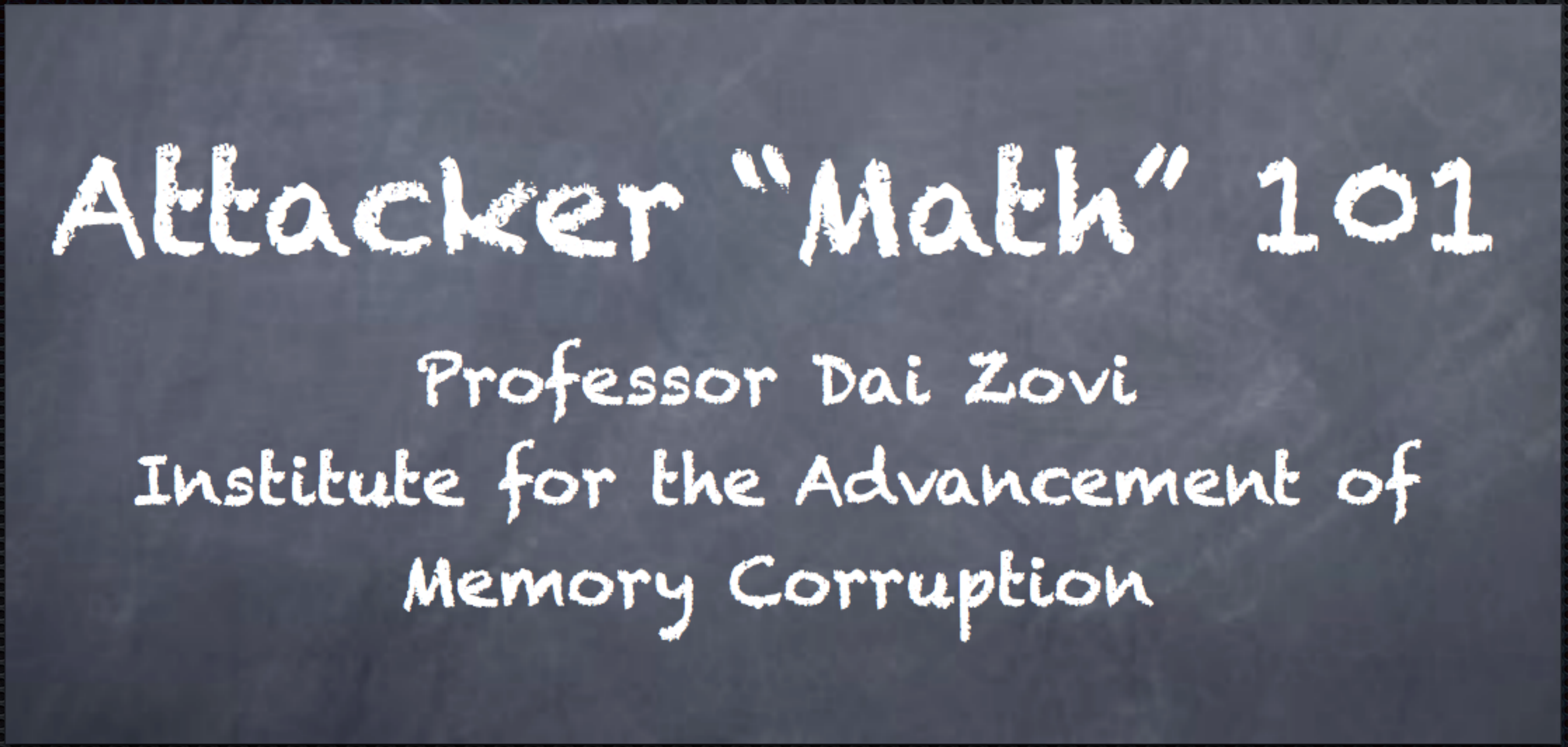
Attackers know Costs



> If the cost to attack is less than the value of your information to the attacker, you will be attacked

Dino Dai Zovi - “Attacker Math” (2011)

	KNOWN	UNKNOWN
ATTACKER	Cost to Attacker Value to Attacker	-
DEFENDER	Value to attacker?	Cost to attacker

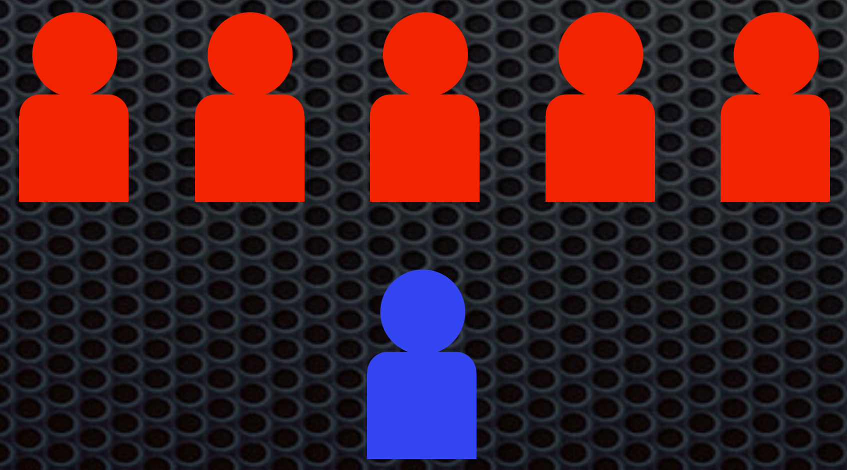


Attacker "Math" 101

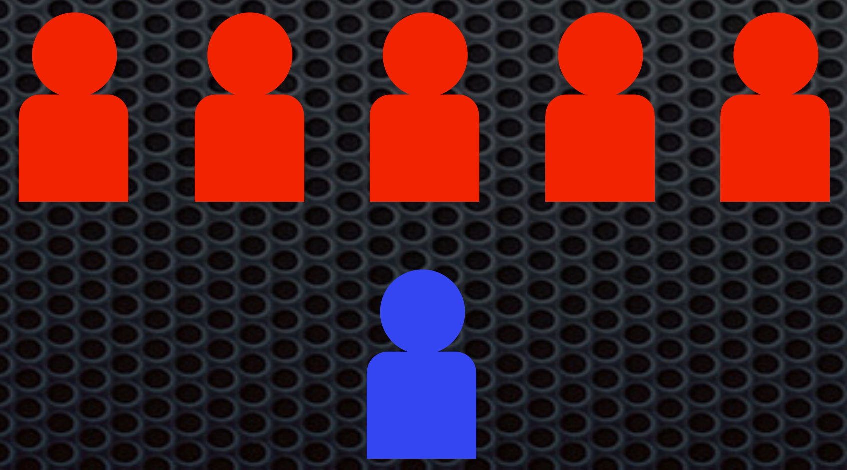
Professor Dai Zovi
Institute for the Advancement of
Memory Corruption

https://web.archive.org/web/20160826071845/https://www.trailofbits.com/resources/attacker_math_101_slides.pdf

Attackers write Code

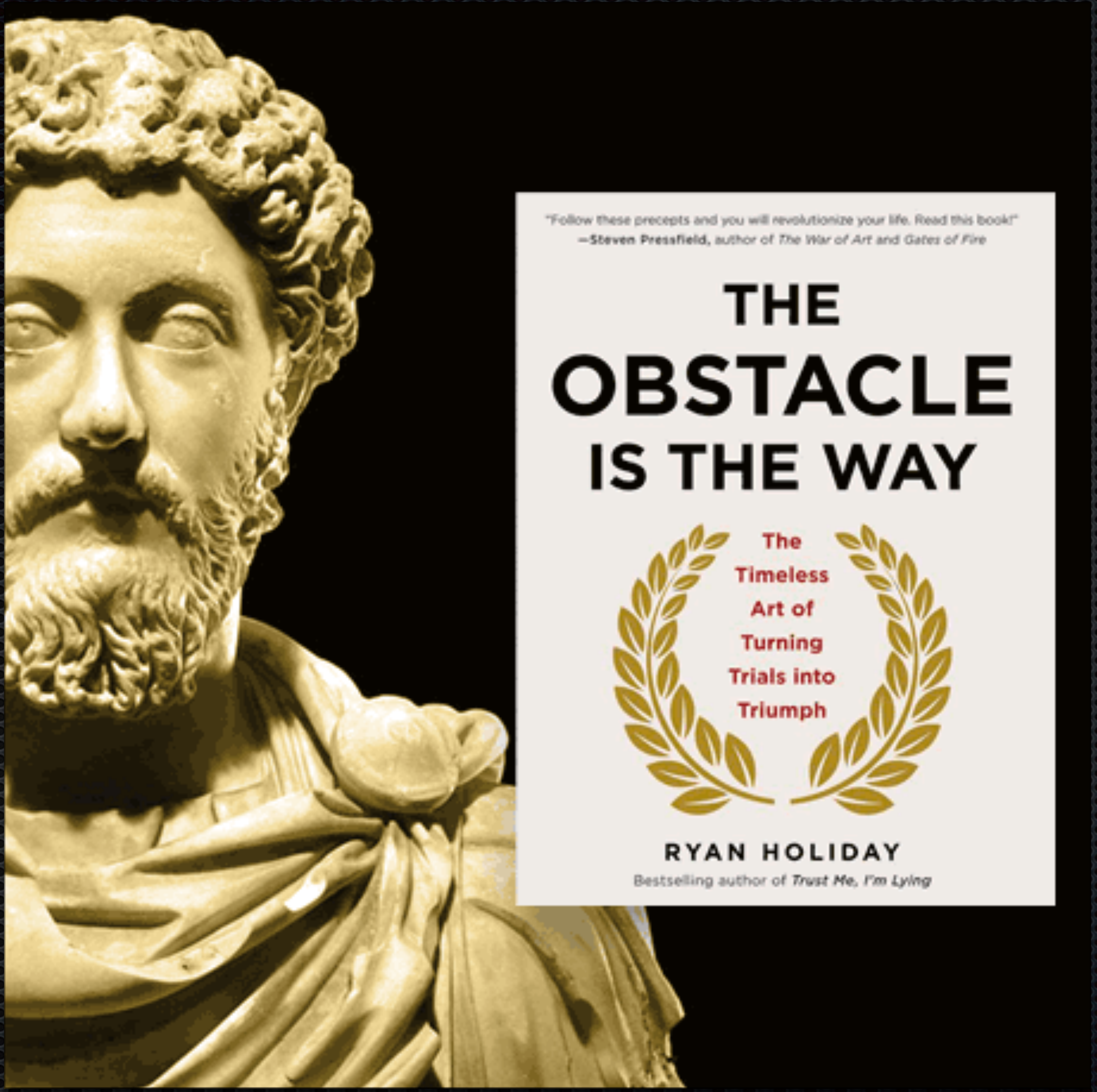


Enterprise Obstacles



Enterprise Obstacles

(our attitudes to them)



"Follow these precepts and you will revolutionize your life. Read this book!"
—**Steven Pressfield,** author of *The War of Art* and *Gates of Fire*

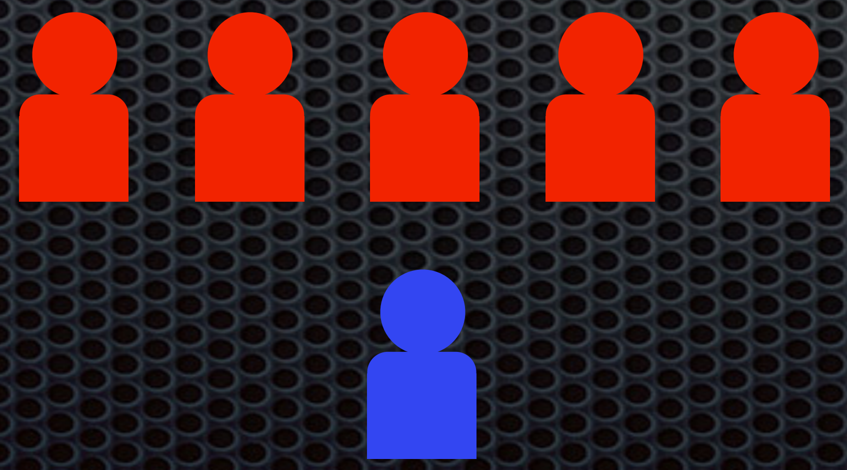
THE OBSTACLE IS THE WAY

The Timeless Art of Turning Trials into Triumph

RYAN HOLIDAY

Bestselling author of ***Trust Me, I'm Lying***

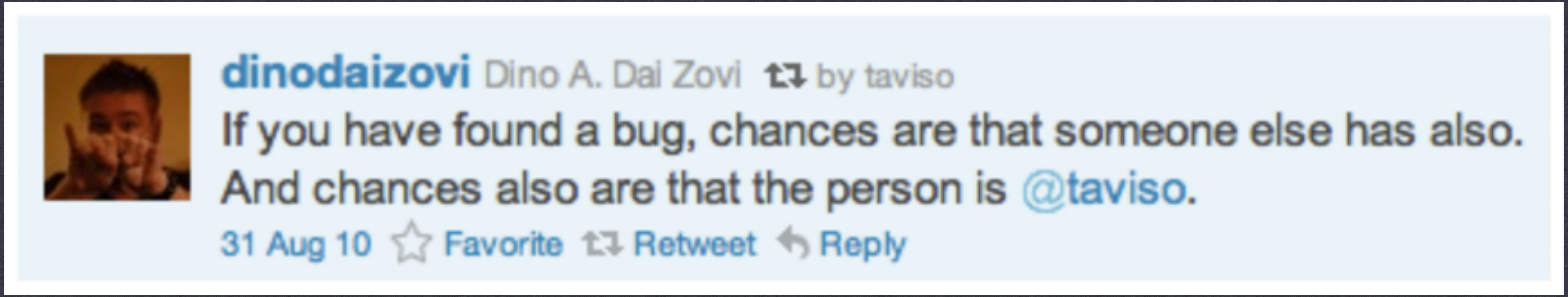
Attack vs. Defense



“It’s always easier for others”

But.. We need to be honest..

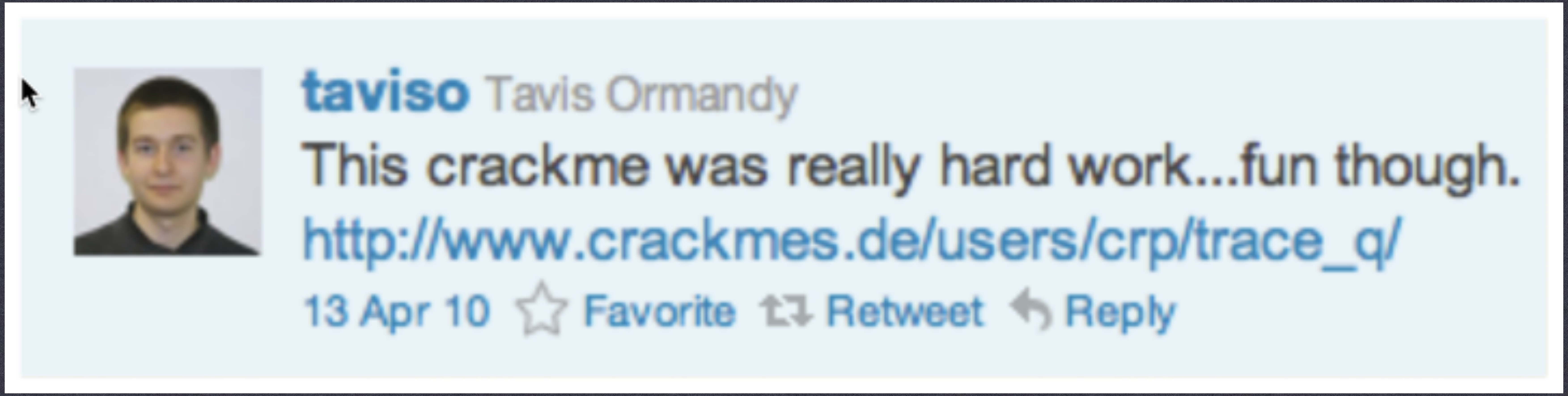
10,000 hours…



dinodaizovi Dino A. Dai Zovi by taviso

If you have found a bug, chances are that someone else has also. And chances also are that the person is @taviso.

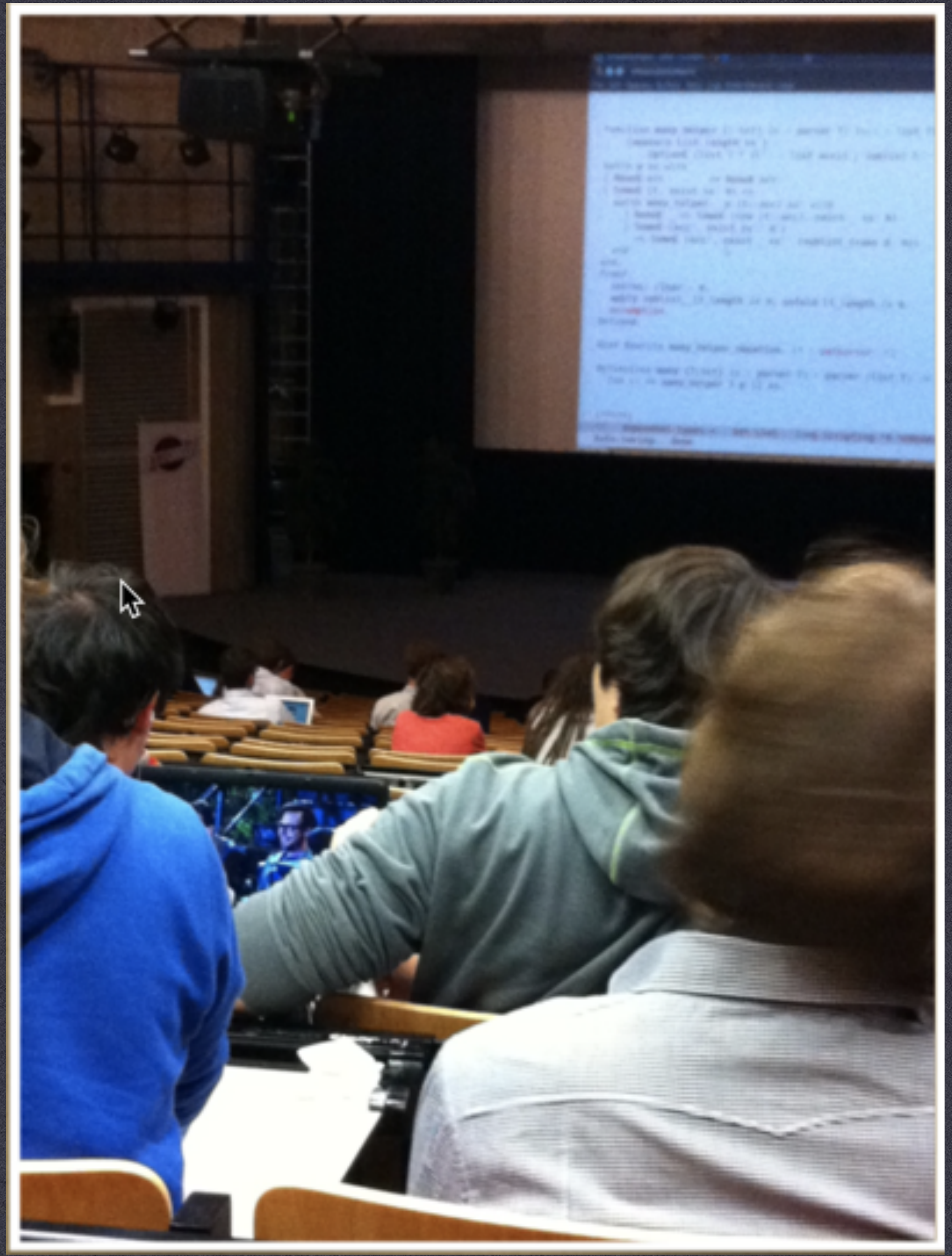
31 Aug 10



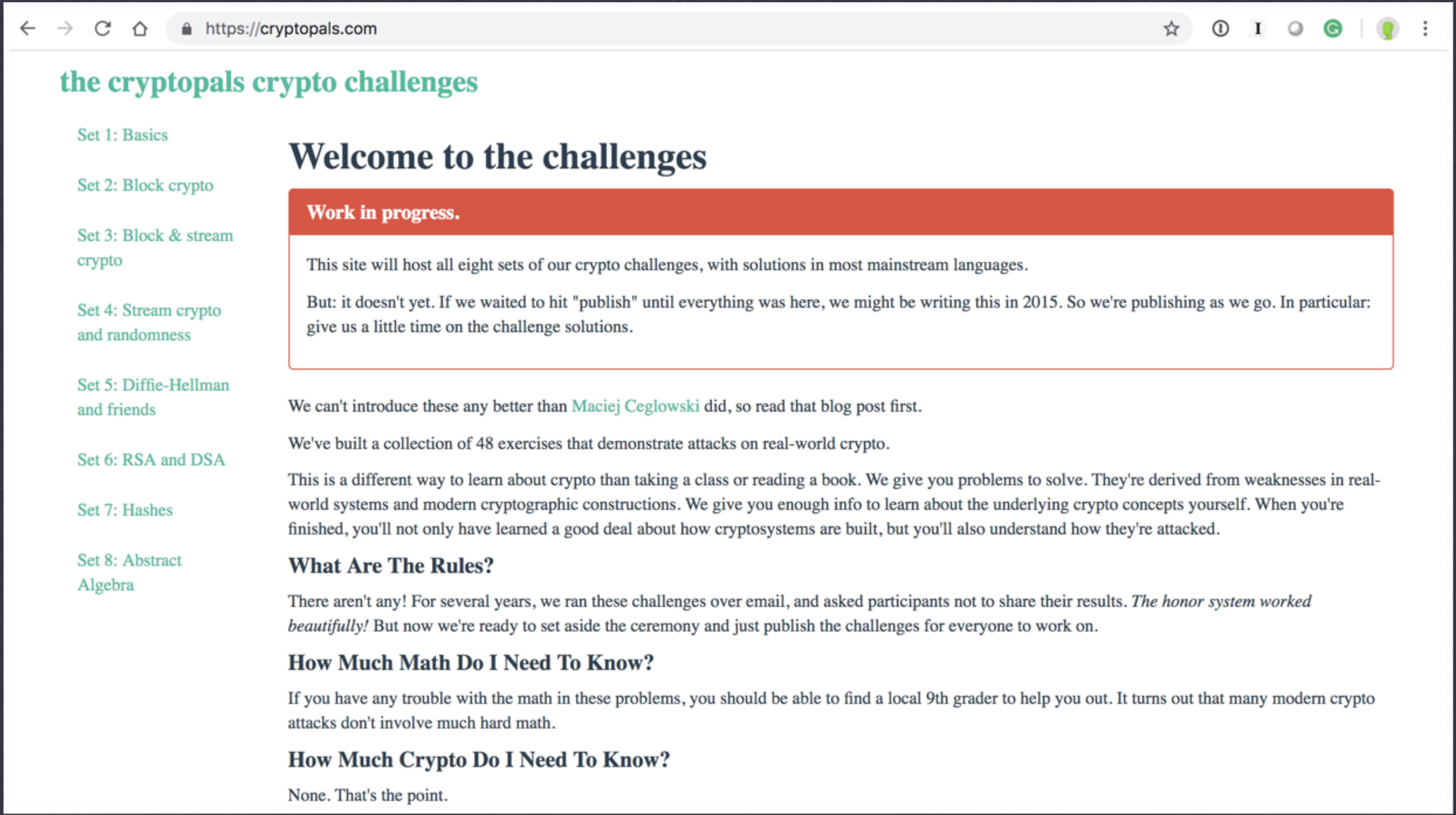
taviso Tavis Ormandy

This crackme was really hard work...fun though. http://www.crackmes.de/users/crp/trace_q/

13 Apr 10



THE
SILVER
BULLET
SECURITY PODCAST
WITH GARY McGRAW
IEEE
SECURITY&PRIVACY
synopsys



the cryptopals crypto challenges

- Set 1: Basics
- Set 2: Block crypto
- Set 3: Block & stream crypto
- Set 4: Stream crypto and randomness
- Set 5: Diffie-Hellman and friends
- Set 6: RSA and DSA
- Set 7: Hashes
- Set 8: Abstract Algebra

Welcome to the challenges

Work in progress.

This site will host all eight sets of our crypto challenges, with solutions in most mainstream languages.

But: it doesn't yet. If we waited to hit "publish" until everything was here, we might be writing this in 2015. So we're publishing as we go. In particular: give us a little time on the challenge solutions.

We can't introduce these any better than Maciej Ceglowski did, so read that blog post first.

We've built a collection of 48 exercises that demonstrate attacks on real-world crypto.

This is a different way to learn about crypto than taking a class or reading a book. We give you problems to solve. They're derived from weaknesses in real-world systems and modern cryptographic constructions. We give you enough info to learn about the underlying crypto concepts yourself. When you're finished, you'll not only have learned a good deal about how cryptosystems are built, but you'll also understand how they're attacked.

What Are The Rules?

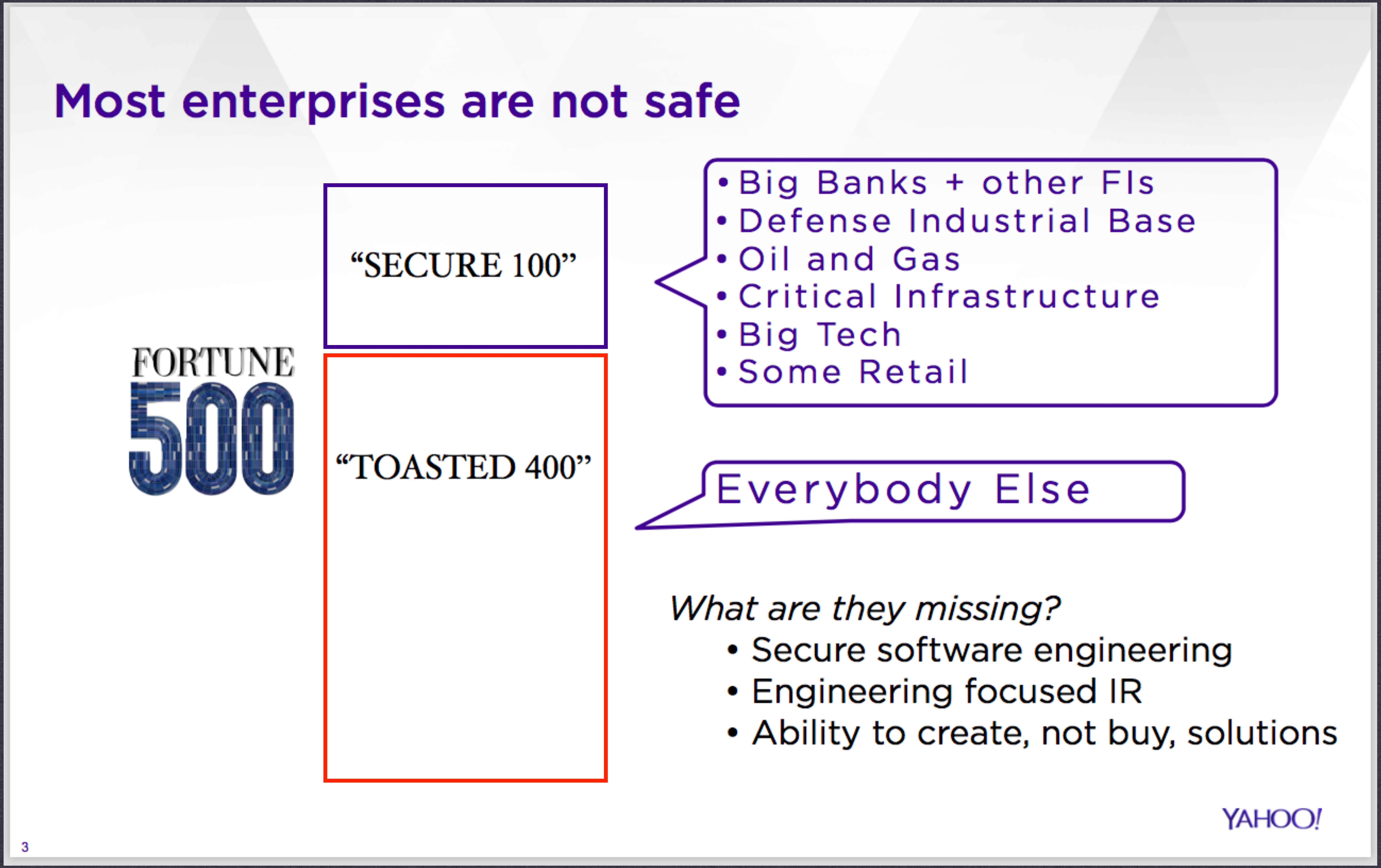
There aren't any! For several years, we ran these challenges over email, and asked participants not to share their results. *The honor system worked beautifully!* But now we're ready to set aside the ceremony and just publish the challenges for everyone to work on.

How Much Math Do I Need To Know?

If you have any trouble with the math in these problems, you should be able to find a local 9th grader to help you out. It turns out that many modern crypto attacks don't involve much hard math.

How Much Crypto Do I Need To Know?

None. That's the point.



Most enterprises are not safe

FORTUNE 500

“SECURE 100”

- Big Banks + other FIs
- Defense Industrial Base
- Oil and Gas
- Critical Infrastructure
- Big Tech
- Some Retail

“TOASTED 400”

Everybody Else

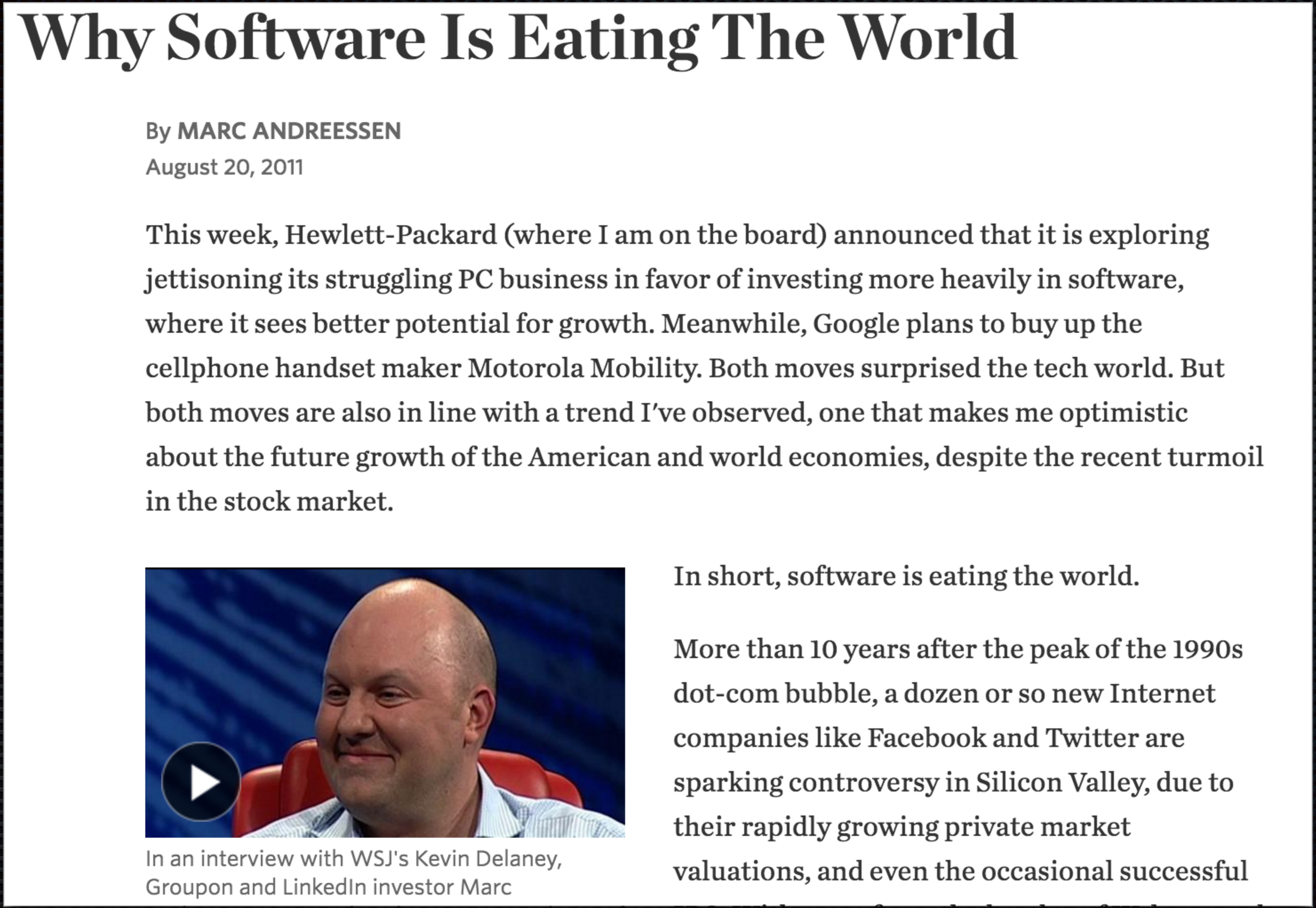
What are they missing?

- Secure software engineering
- Engineering focused IR
- Ability to create, not buy, solutions

YAHOO!

3

https://www.slideshare.net/astamos/appsec-is-eating-security



Why Software Is Eating The World

By MARC ANDREESSEN
August 20, 2011

This week, Hewlett-Packard (where I am on the board) announced that it is exploring jettisoning its struggling PC business in favor of investing more heavily in software, where it sees better potential for growth. Meanwhile, Google plans to buy up the cellphone handset maker Motorola Mobility. Both moves surprised the tech world. But both moves are also in line with a trend I've observed, one that makes me optimistic about the future growth of the American and world economies, despite the recent turmoil in the stock market.

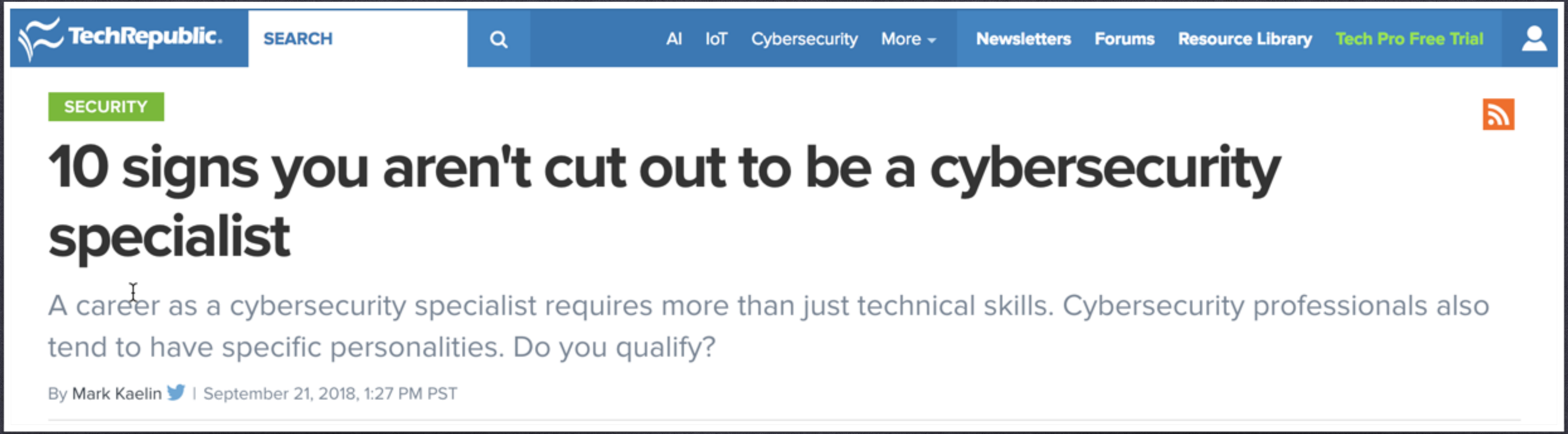
In an interview with WSJ's Kevin Delaney, Groupon and LinkedIn investor Marc

In short, software is eating the world.

More than 10 years after the peak of the 1990s dot-com bubble, a dozen or so new Internet companies like Facebook and Twitter are sparking controversy in Silicon Valley, due to their rapidly growing private market valuations, and even the occasional successful

http://www.wsj.com/articles/SB10001424053111903480904576512250915629460

Super easy to be nihilistic



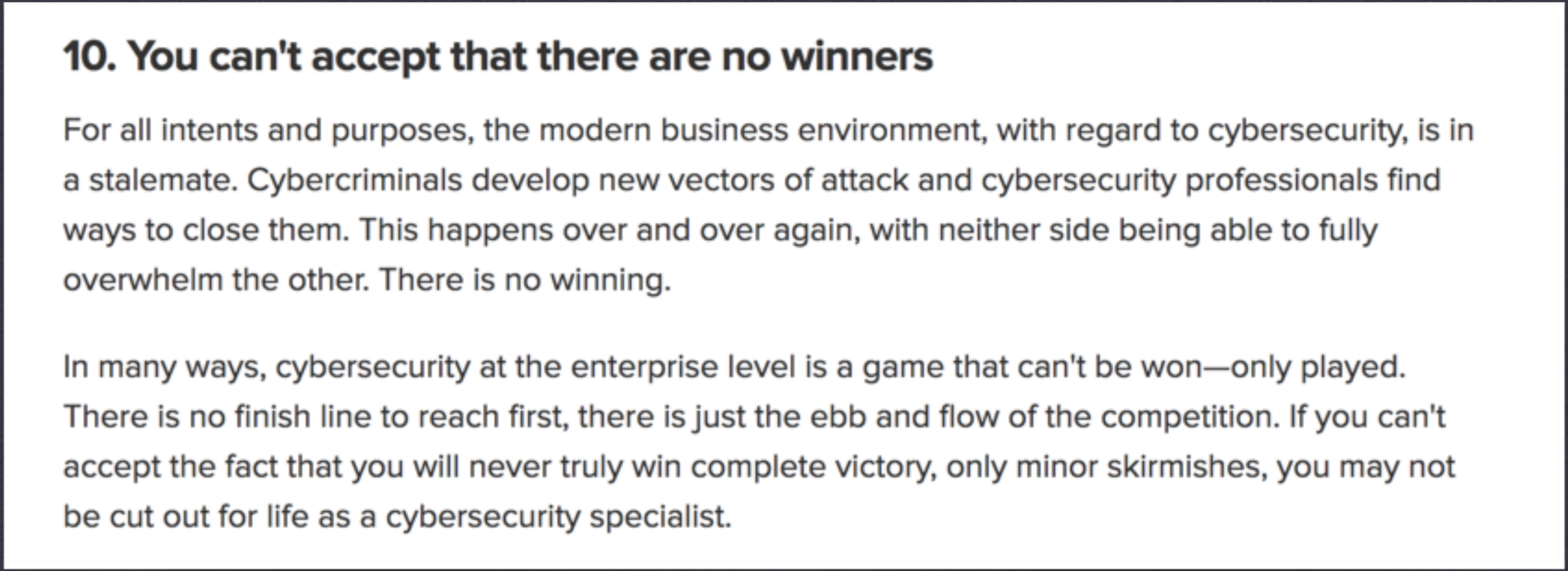
SECURITY

10 signs you aren't cut out to be a cybersecurity specialist

A career as a cybersecurity specialist requires more than just technical skills. Cybersecurity professionals also tend to have specific personalities. Do you qualify?

By Mark Kaelin | September 21, 2018, 1:27 PM PST

https://www.techrepublic.com/article/10-signs-you-arent-cut-out-to-be-a-cybersecurity-specialist/



10. You can't accept that there are no winners

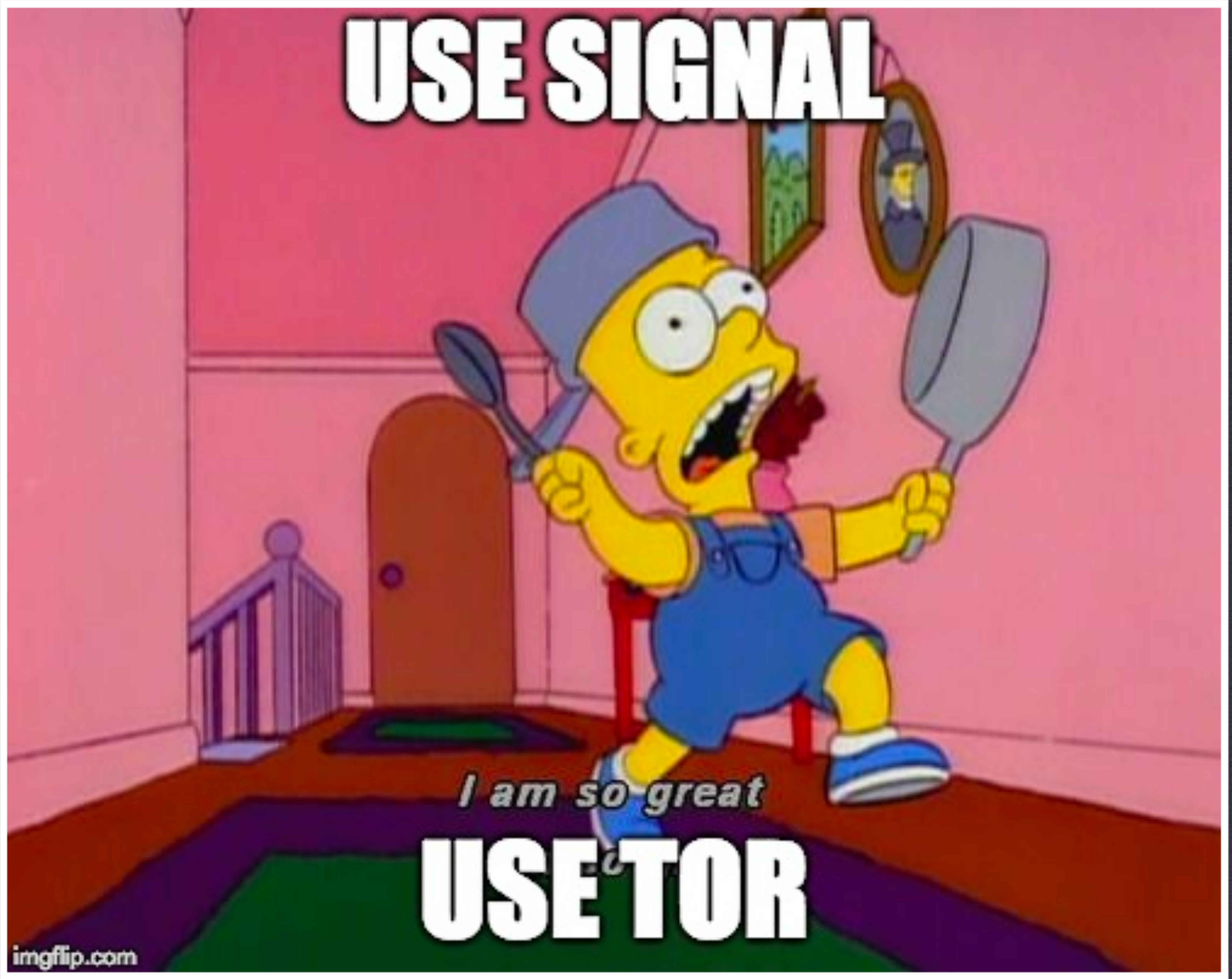
For all intents and purposes, the modern business environment, with regard to cybersecurity, is in a stalemate. Cybercriminals develop new vectors of attack and cybersecurity professionals find ways to close them. This happens over and over again, with neither side being able to fully overwhelm the other. There is no winning.

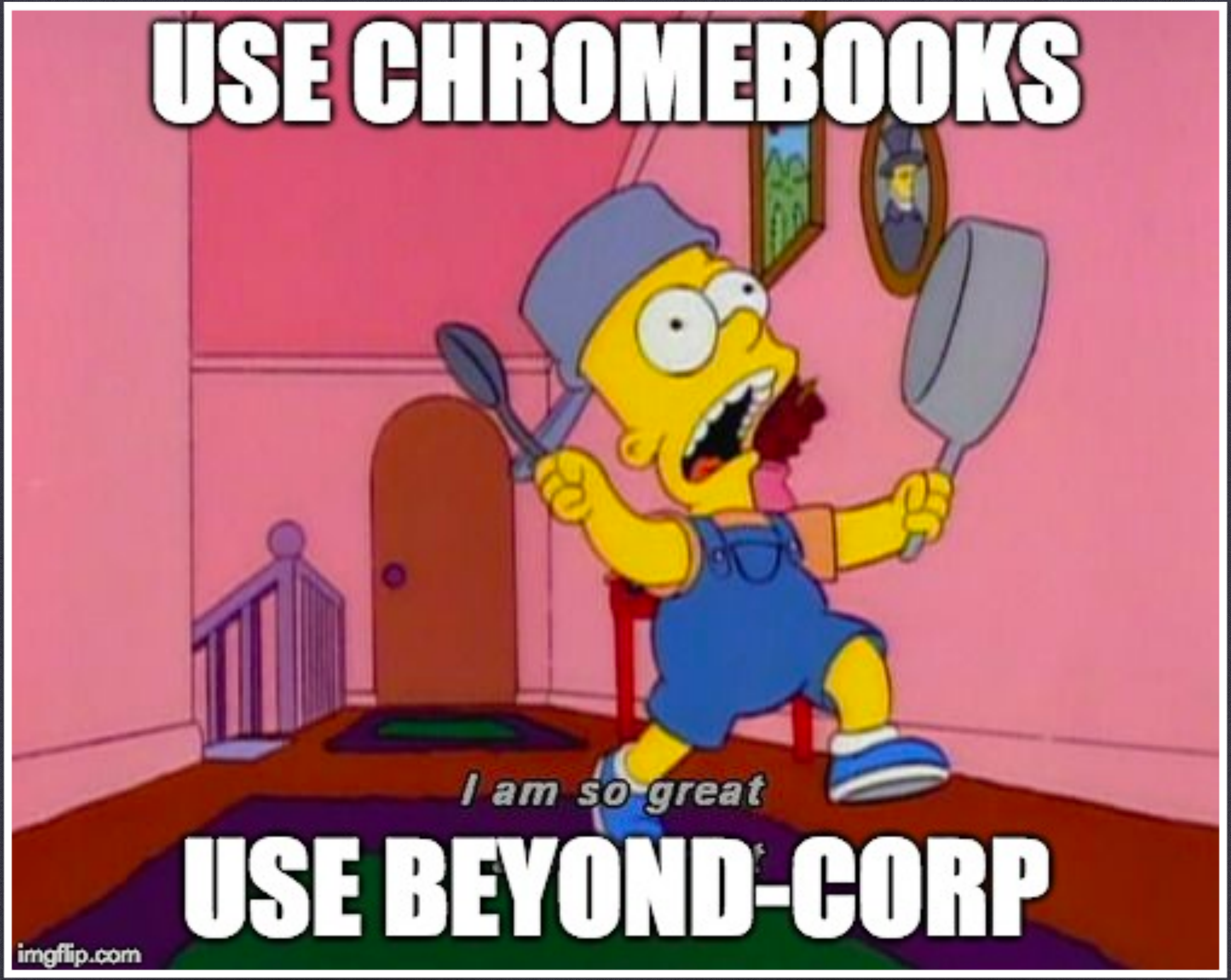
In many ways, cybersecurity at the enterprise level is a game that can't be won—only played. There is no finish line to reach first, there is just the ebb and flow of the competition. If you can't accept the fact that you will never truly win complete victory, only minor skirmishes, you may not be cut out for life as a cybersecurity specialist.

https://www.techrepublic.com/article/10-signs-you-arent-cut-out-to-be-a-cybersecurity-specialist/

p@#! - or get off the pot!

ALMOST ALL GENERIC ADVICE IS WRONG


USE SIGNAL
I am so great
USE TOR
imgflip.com


USE CHROMEBOOKS
I am so great
USE BEYOND-CORP
imgflip.com

SECURITY

BeyondCorp

A New Approach to Enterprise Security

RORY WARD AND BETSY BEYER

Rory Ward is a site reliability engineering manager in Google Ireland. He previously worked in Ireland at Valista, in Silicon Valley at AOL, Netscape, Kiva, and General Magic, and in Los Angeles at Retix. He has a BSc in computer applications from Dublin City University. roryward@google.com

Betsy Beyer is a technical writer specializing in virtualization software for Google SRE in NYC. She has previously provided documentation for Google Data Center and Hardware Operations teams. Before moving to New York, Betsy was a lecturer in technical writing at Stanford University. She holds degrees from Stanford and Tulane. bbeyer@google.com

Virtually every company today uses firewalls to enforce perimeter security. However, this security model is problematic because, when that perimeter is breached, an attacker has relatively easy access to a company's privileged intranet. As companies adopt mobile and cloud technologies, the perimeter is becoming increasingly difficult to enforce. Google is taking a different approach to network security. We are removing the requirement for a privileged intranet and moving our corporate applications to the Internet.

Since the early days of IT infrastructure, enterprises have used perimeter security to protect and gate access to internal resources. The perimeter security model is often compared to a medieval castle: a fortress with thick walls, surrounded by a moat, with a heavily guarded single point of entry and exit. Anything located outside the wall is considered dangerous, while anything located inside the wall is trusted. Anyone who makes it past the drawbridge has ready access to the resources of the castle.

The perimeter security model works well enough when all employees work exclusively in buildings owned by an enterprise. However, with the advent of a mobile workforce, the surge in the variety of devices used by this workforce, and the growing use of cloud-based services, additional attack vectors have emerged that are stretching the traditional paradigm to the point of redundancy. Key assumptions of this model no longer hold: The perimeter is no longer just the physical location of the enterprise, and what lies inside the perimeter is no longer a blessed and safe place to host personal computing devices and enterprise applications.

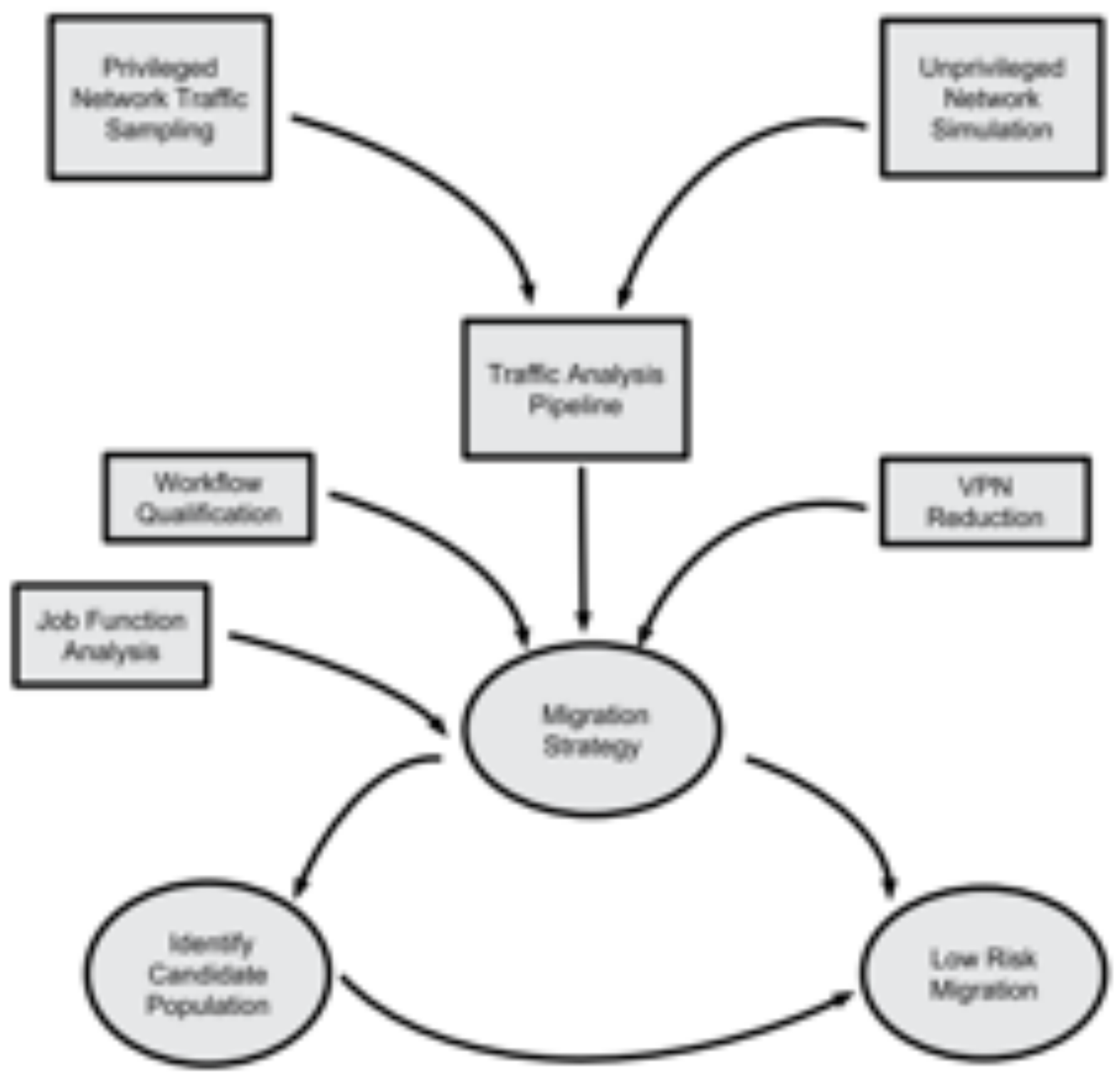

Privileged Network Traffic Sampling
Unprivileged Network Simulation
Traffic Analysis Pipeline
Workflow Qualification
VPN Reduction
Job Function Analysis
Migration Strategy
Identify Candidate Population
Low Risk Migration

Figure 2: Migrating to BeyondCorp

https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf “we take a risk based approach”

How do you test your assumptions?

In many ways, the work of a critic is easy. We risk very little, yet enjoy a position over those who offer up their work and their selves to our judgment. We thrive on negative criticism, which is fun to write and to read. But the bitter truth we critics must face is that, in the grand scheme of things, the average piece of junk is probably more meaningful than our criticism designating it so. But there are times when a critic truly risks something, and that is in the discovery and defense of the new. The world is often unkind to new talent, new creations. The new needs friends.

Modern CISO is in a powerful position

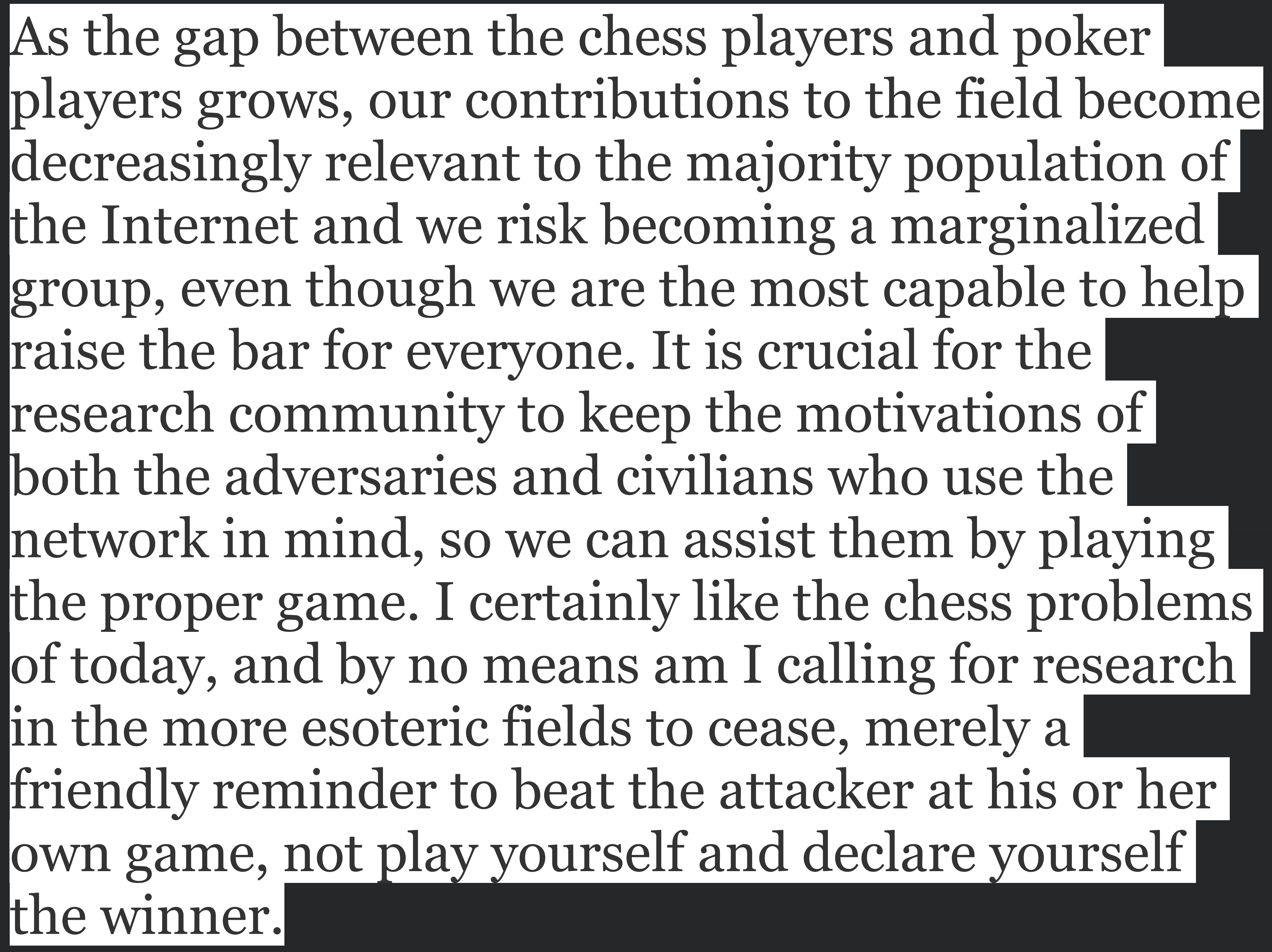
Security Researchers

Chess Vs. Poker

Or: why we’re playing the wrong game

Jacob Torrey

Cyber-security Philosopher and Boffin



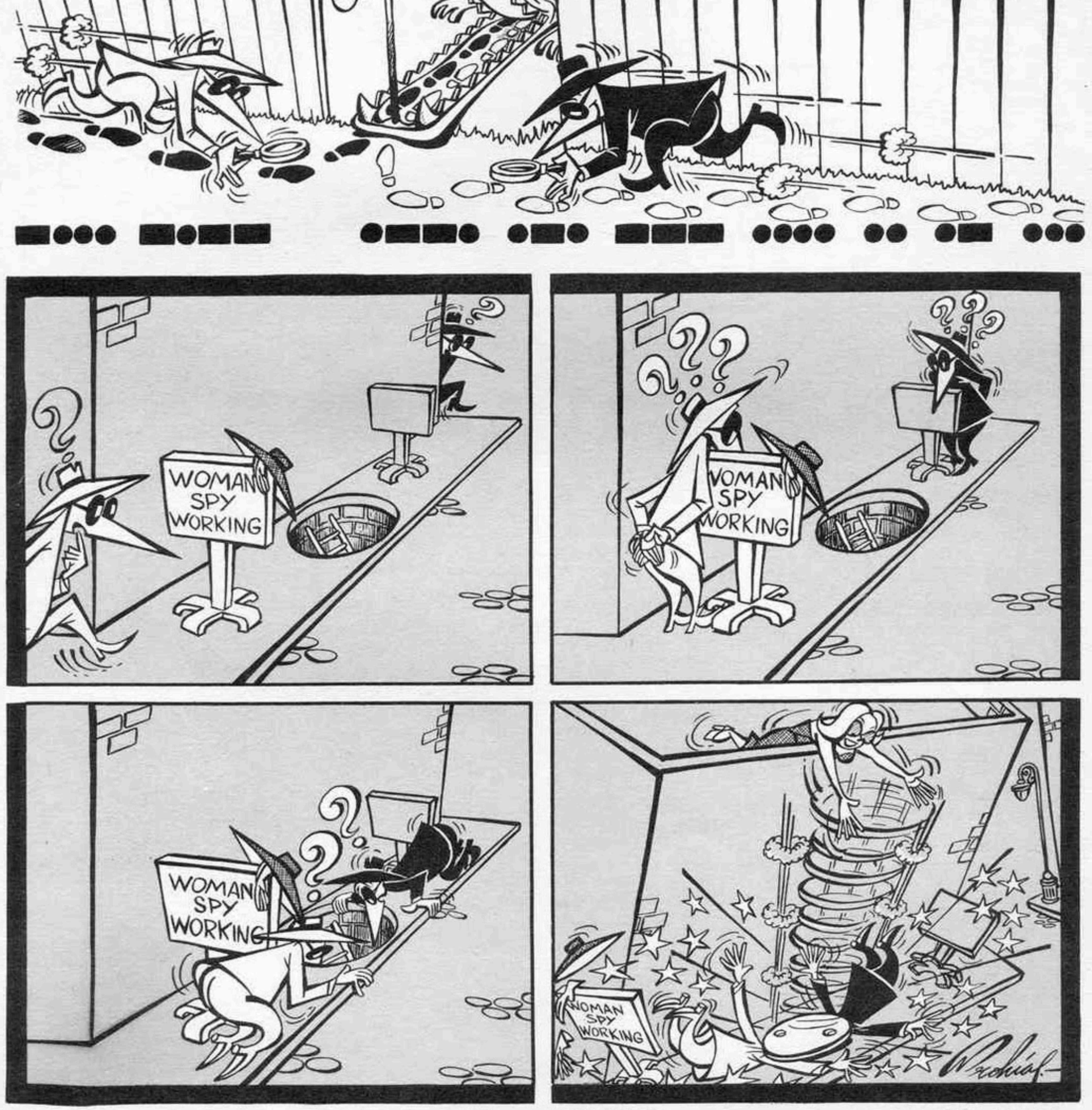
As the gap between the chess players and poker players grows, our contributions to the field become decreasingly relevant to the majority population of the Internet and we risk becoming a marginalized group, even though we are the most capable to help raise the bar for everyone. It is crucial for the research community to keep the motivations of both the adversaries and civilians who use the network in mind, so we can assist them by playing the proper game. I certainly like the chess problems of today, and by no means am I calling for research in the more esoteric fields to cease, merely a friendly reminder to beat the attacker at his or her own game, not play yourself and declare yourself the winner.

http://blog.jacobtorrey.com/chess-vs-poker

Apple Security - “LOL”

“When we win it's with small things,
and the triumph itself makes us small”

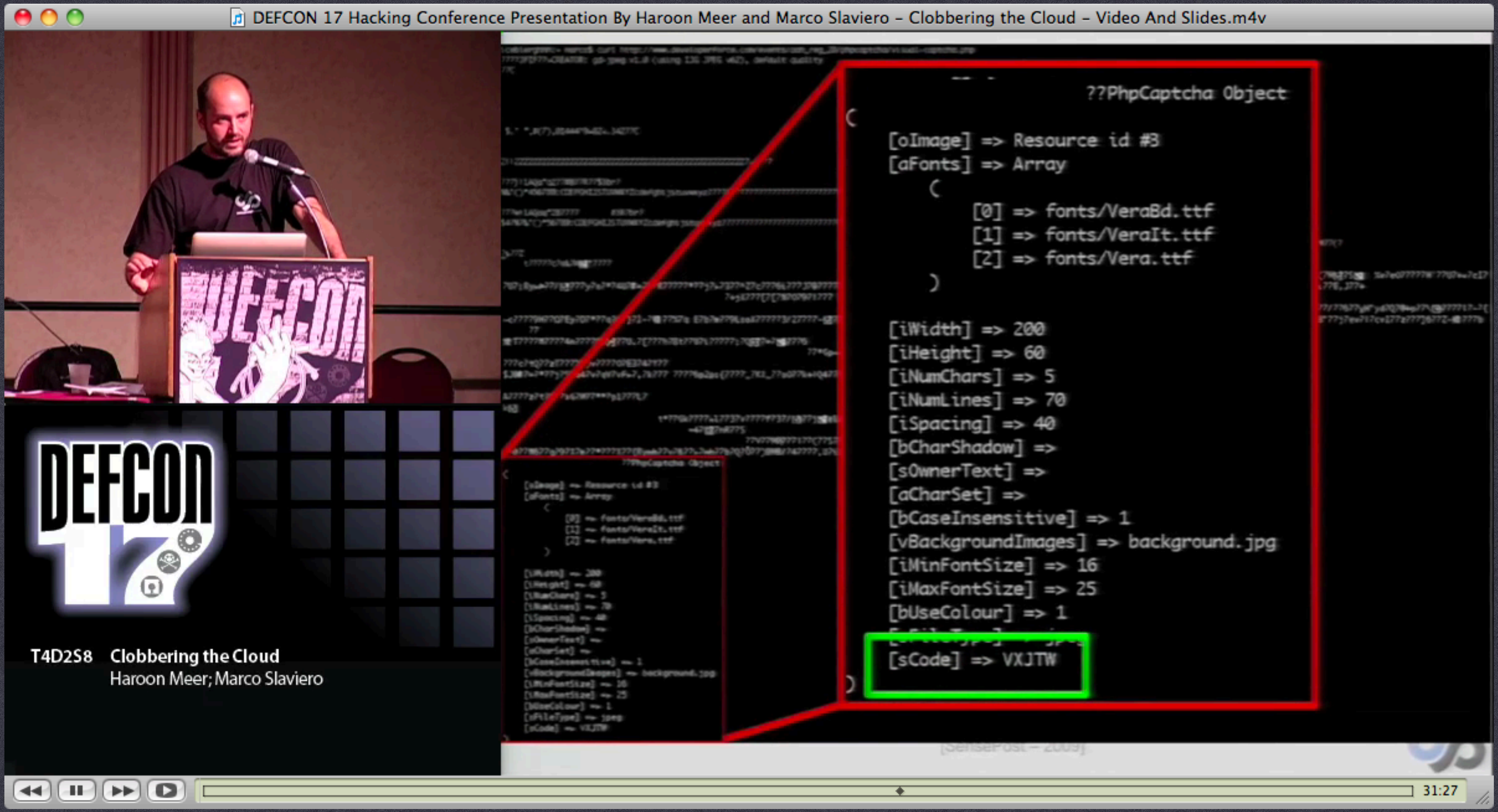
http://www.michaelppowers.com/wisdom/rilke.html


WOMAN SPY WORKING
WOMAN SPY WORKING
WOMAN SPY WORKING
WOMAN SPY WORKING
Prohias

CANDID CAMERA

When the
Tables
Turn
REVENGE IS A DISH BEST SERVED COLD
sensepost

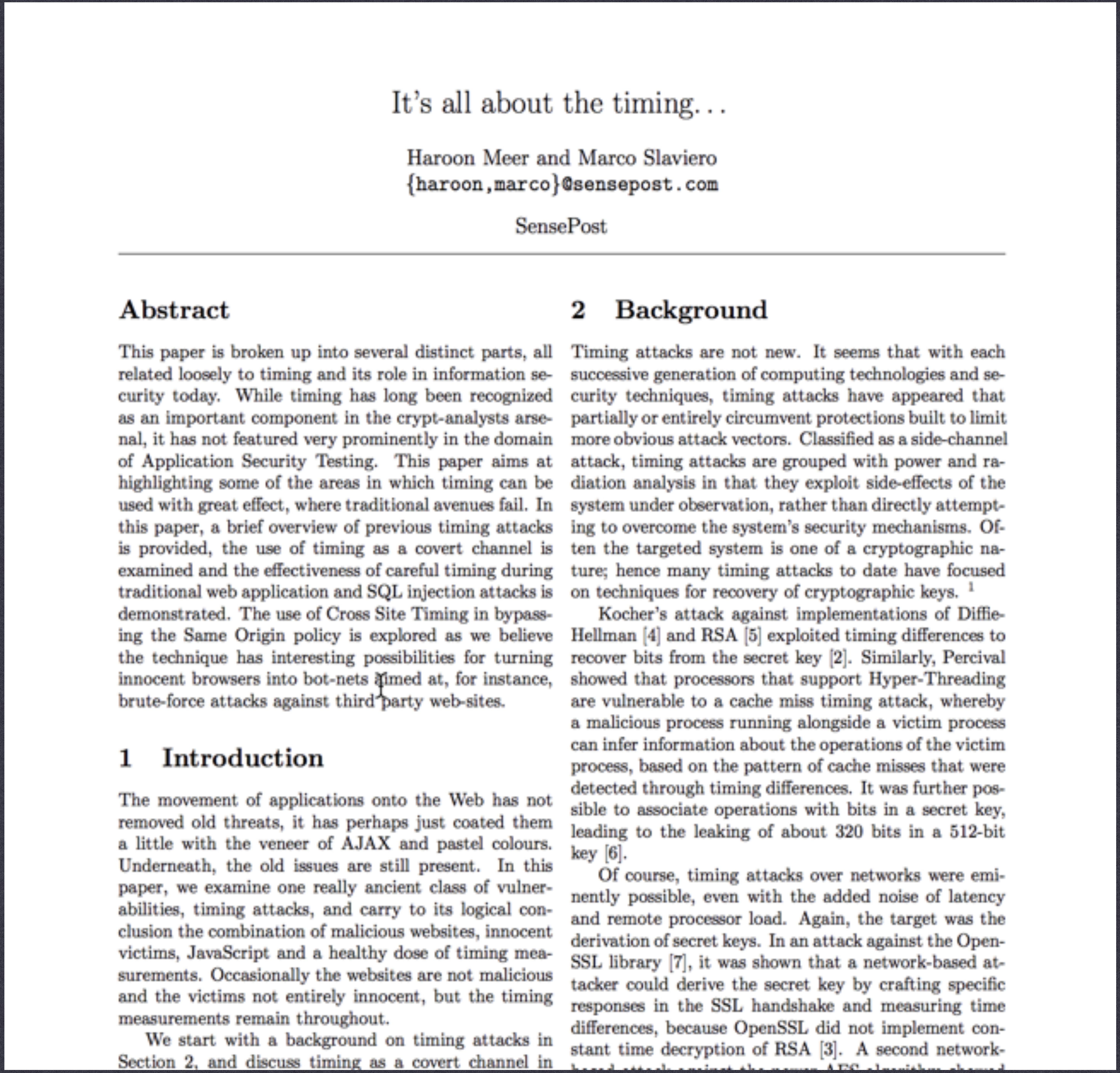
f


DEFCON 17 Hacking Conference Presentation By Haroon Meer and Marco Slaviero – Clobbering the Cloud – Video And Slides.m4v
DEFCON 17
T4D2S8 Clobbering the Cloud
Haroon Meer; Marco Slaviero
31:27

```
                              ??PhpCaptcha Object
(
    [oImage] => Resource id #3
    [aFonts] => Array
        (
            [0] => fonts/VeraBd.ttf
            [1] => fonts/VeraIt.ttf
            [2] => fonts/Vera.ttf
        )

    [iWidth] => 200
    [iHeight] => 60
    [iNumChars] => 5
    [iNumLines] => 70
    [iSpacing] => 40
    [bCharShadow] =>
    [sOwnerText] =>
    [aCharSet] =>
    [bCaseInsensitive] => 1
    [vBackgroundImages] => background.jpg
    [iMinFontSize] => 16
    [iMaxFontSize] => 25
    [bUseColour] => 1
    [sFileType] => jpeg
    [sCode] => VXJTW
)
```

UBER



It's all about the timing...

Haroon Meer and Marco Slaviero
{haroon,marco}@sensepost.com

SensePost

Abstract

This paper is broken up into several distinct parts, all related loosely to timing and its role in information security today. While timing has long been recognized as an important component in the crypt-analysts arsenal, it has not featured very prominently in the domain of Application Security Testing. This paper aims at highlighting some of the areas in which timing can be used with great effect, where traditional avenues fail. In this paper, a brief overview of previous timing attacks is provided, the use of timing as a covert channel is examined and the effectiveness of careful timing during traditional web application and SQL injection attacks is demonstrated. The use of Cross Site Timing in bypassing the Same Origin policy is explored as we believe the technique has interesting possibilities for turning innocent browsers into bot-nets aimed at, for instance, brute-force attacks against third party web-sites.

1 Introduction

The movement of applications onto the Web has not removed old threats, it has perhaps just coated them a little with the veneer of AJAX and pastel colours. Underneath, the old issues are still present. In this paper, we examine one really ancient class of vulnerabilities, timing attacks, and carry to its logical conclusion the combination of malicious websites, innocent victims, JavaScript and a healthy dose of timing measurements. Occasionally the websites are not malicious and the victims not entirely innocent, but the timing measurements remain throughout.

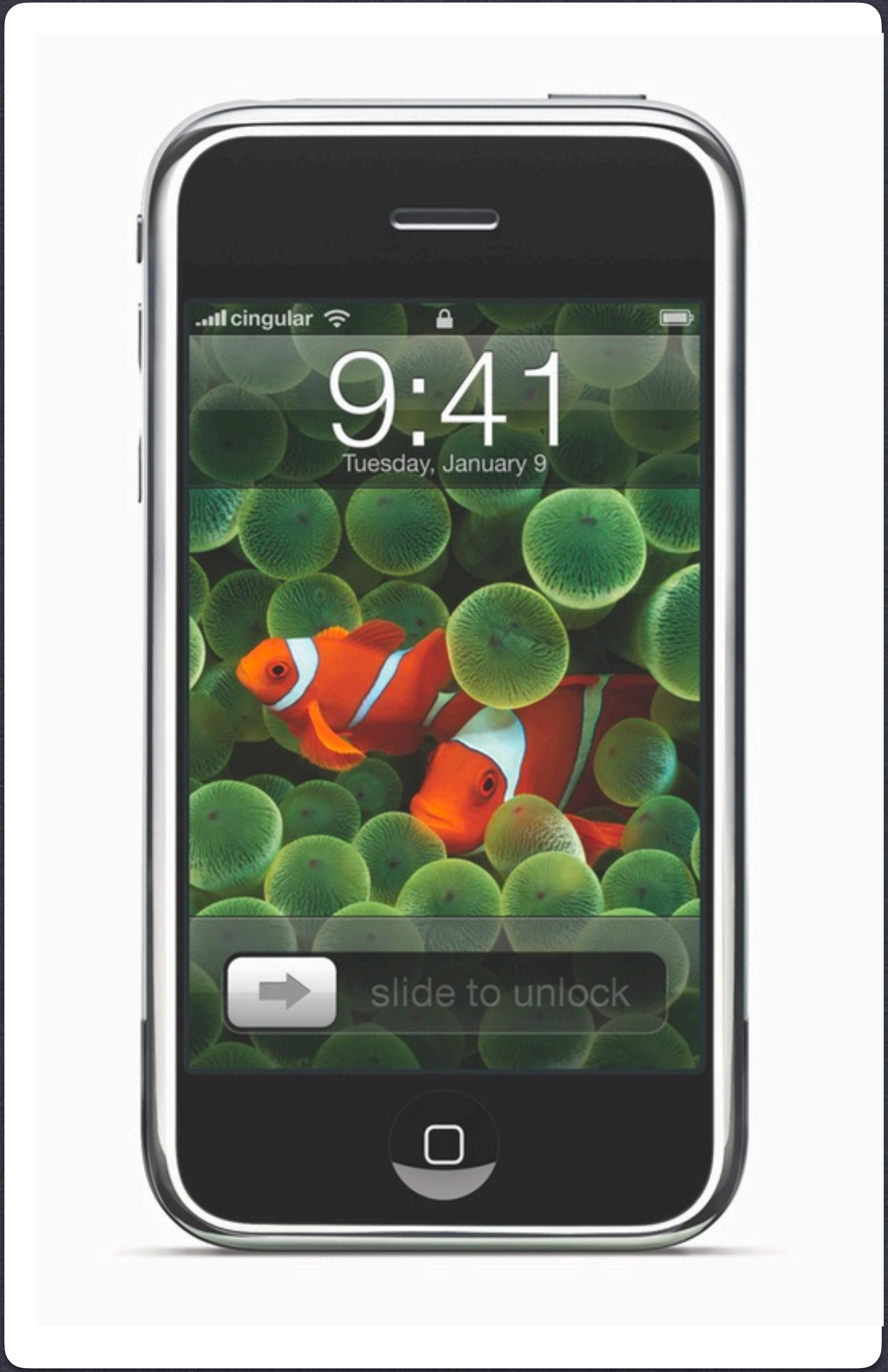
We start with a background on timing attacks in Section 2, and discuss timing as a covert channel in

2 Background

Timing attacks are not new. It seems that with each successive generation of computing technologies and security techniques, timing attacks have appeared that partially or entirely circumvent protections built to limit more obvious attack vectors. Classified as a side-channel attack, timing attacks are grouped with power and radiation analysis in that they exploit side-effects of the system under observation, rather than directly attempting to overcome the system's security mechanisms. Often the targeted system is one of a cryptographic nature; hence many timing attacks to date have focused on techniques for recovery of cryptographic keys. [1]

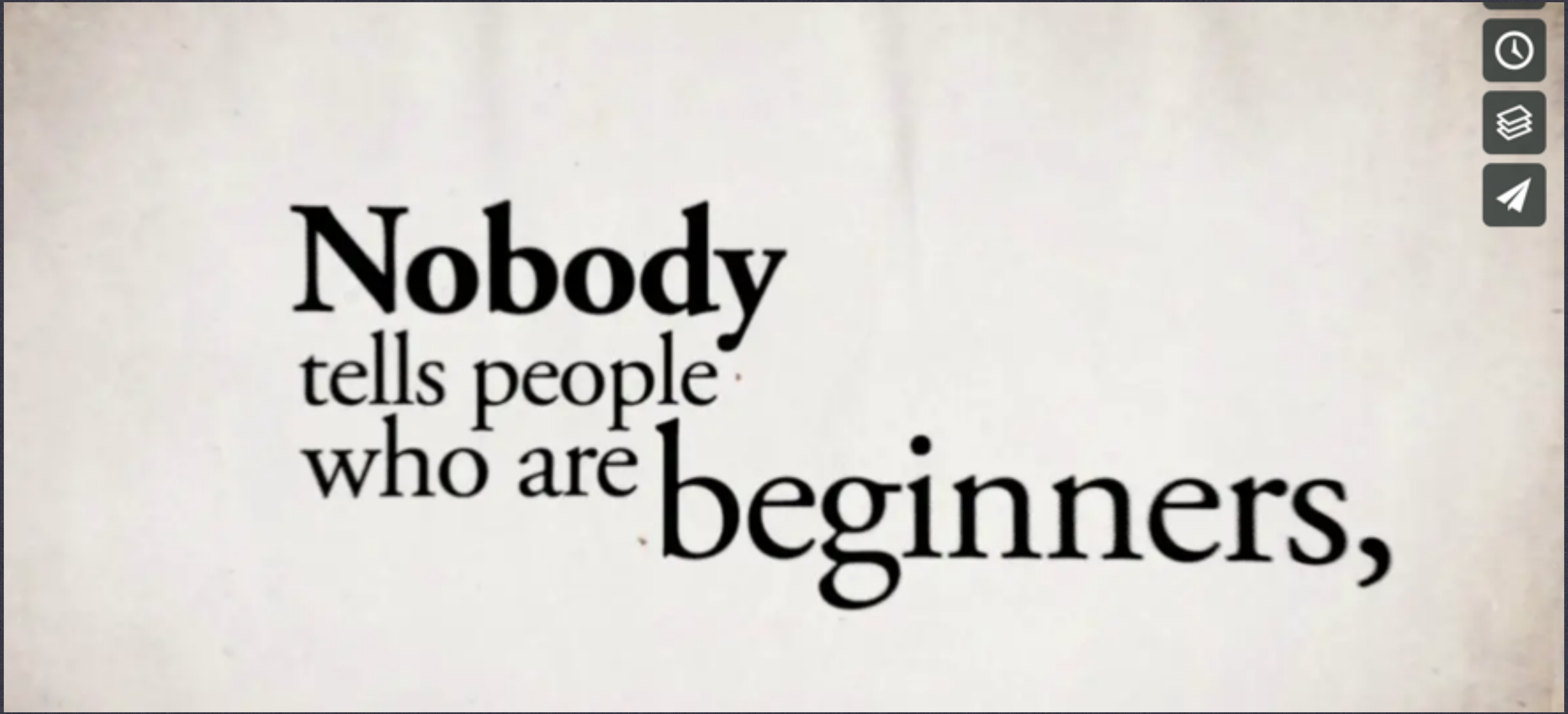
Kocher's attack against implementations of Diffie-Hellman [4] and RSA [5] exploited timing differences to recover bits from the secret key [2]. Similarly, Percival showed that processors that support Hyper-Threading are vulnerable to a cache miss timing attack, whereby a malicious process running alongside a victim process can infer information about the operations of the victim process, based on the pattern of cache misses that were detected through timing differences. It was further possible to associate operations with bits in a secret key, leading to the leaking of about 320 bits in a 512-bit key [6].

Of course, timing attacks over networks were eminently possible, even with the added noise of latency and remote processor load. Again, the target was the derivation of secret keys. In an attack against the OpenSSL library [7], it was shown that a network-based attacker could derive the secret key by crafting specific responses in the SSL handshake and measuring time differences, because OpenSSL did not implement constant time decryption of RSA [3]. A second network-



Make Stuff..

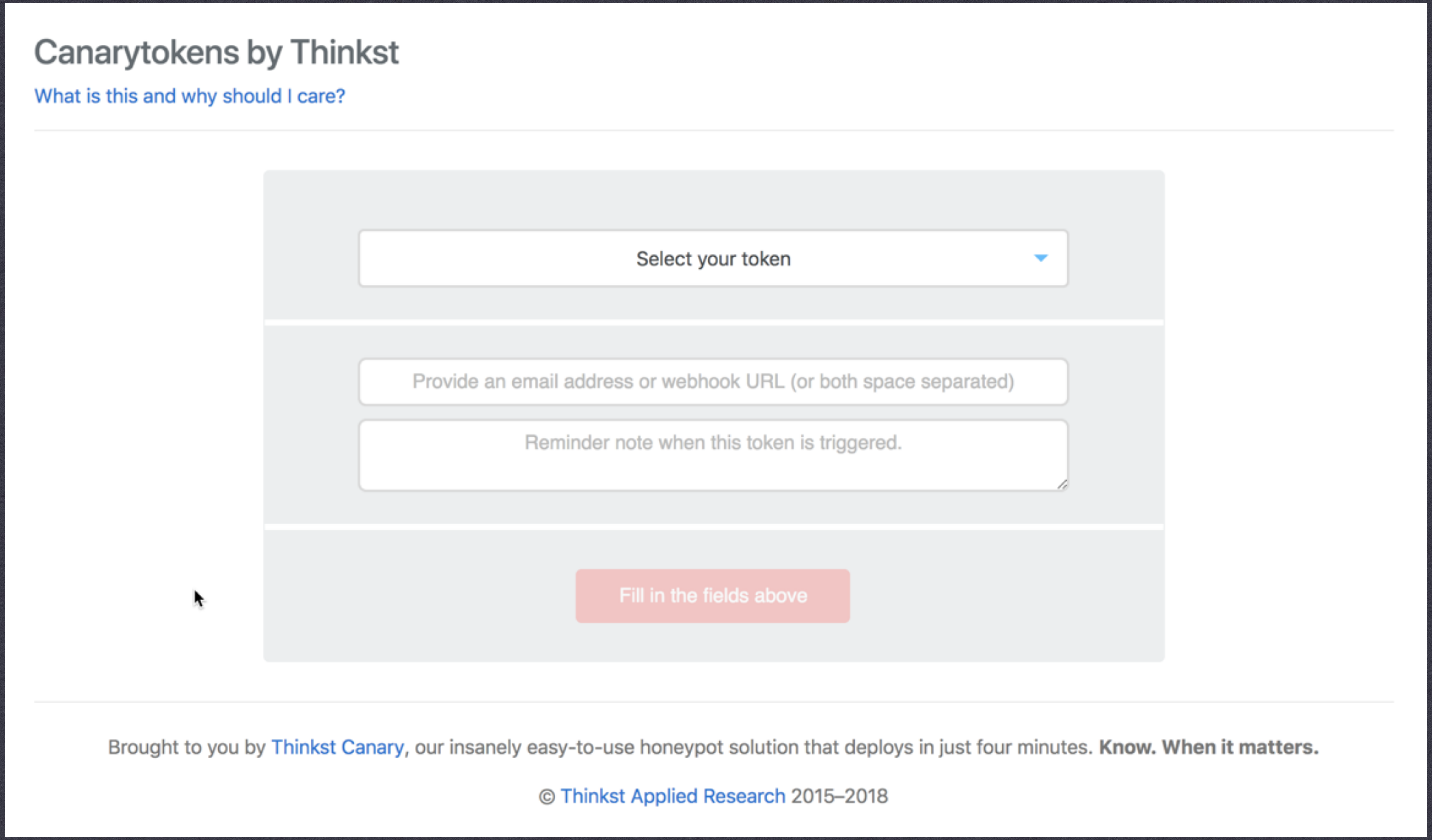
> “when you don't create things, you become defined by your tastes rather than ability. your tastes only narrow & exclude people. so create.”
>
> – **Why The Lucky Stiff**



Nobody tells people who are beginners,

https://vimeo.com/24715531

“Nobody tells this to people who are beginners, I wish someone told me. All of us who do creative work, we get into it because we have good taste. But there is this gap. For the first couple years you make stuff, it’s just not that good. It’s trying to be good, it has potential, but it’s not. But your taste, the thing that got you into the game, is still killer. And your taste is why your work disappoints you. A lot of people never get past this phase, they quit. Most people I know who do interesting, creative work went through years of this. We know our work doesn’t have this special thing that we want it to have. We all go through this. And if you are just starting out or you are still in this phase, you gotta know its normal and the most important thing you can do is do a lot of work. Put yourself on a deadline so that every week you will finish one story. It is only by going through a volume of work that you will close that gap, and your work will be as good as your ambitions. And I took longer to figure out how to do this than anyone I’ve ever met. It’s gonna take awhile. It’s normal to take awhile. You’ve just gotta fight your way through.”



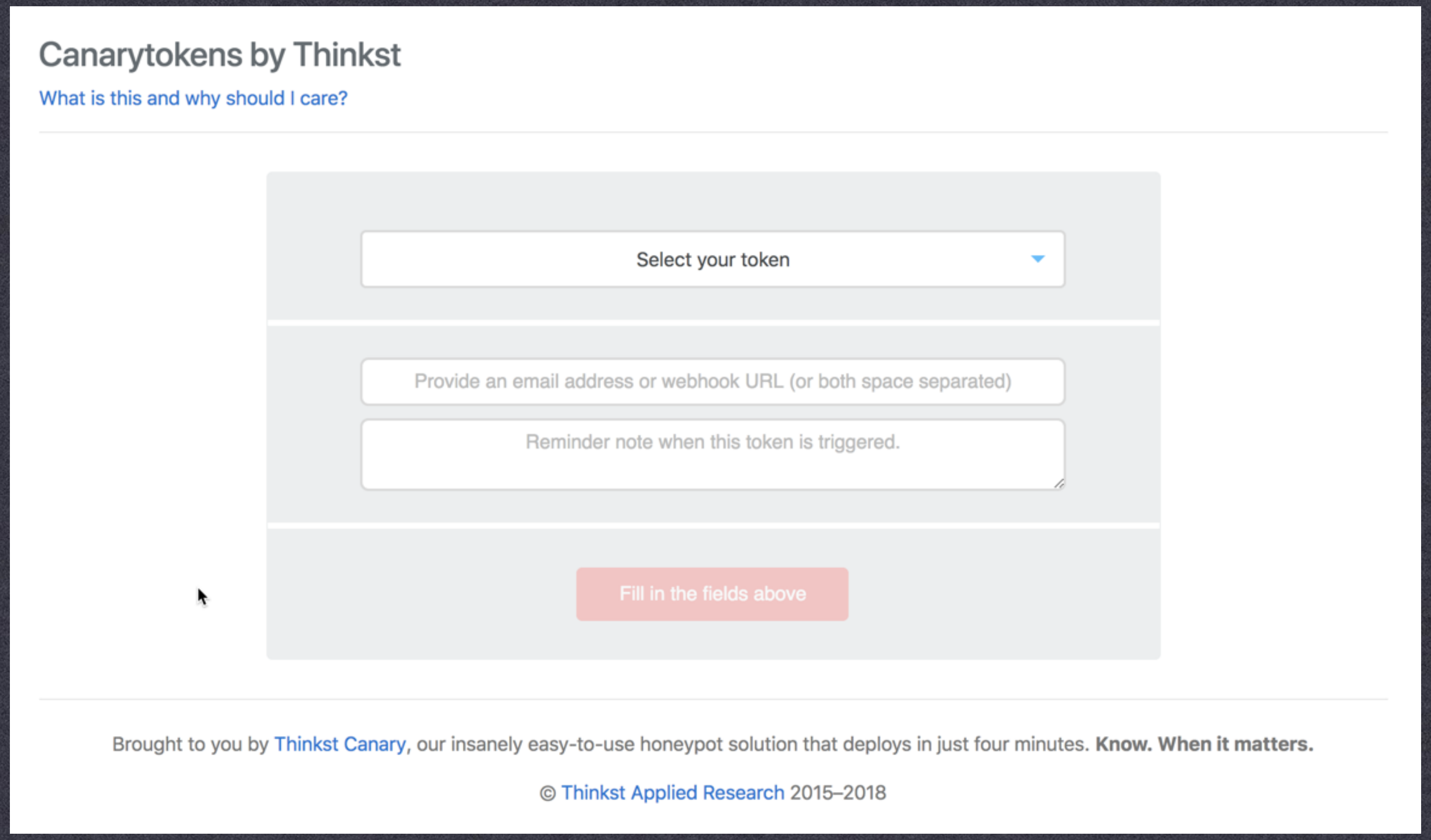
Canarytokens by Thinkst

What is this and why should I care?

Select your token
Provide an email address or webhook URL (or both space separated)
Reminder note when this token is triggered.
Fill in the fields above

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. **Know. When it matters.**

© Thinkst Applied Research 2015–2018



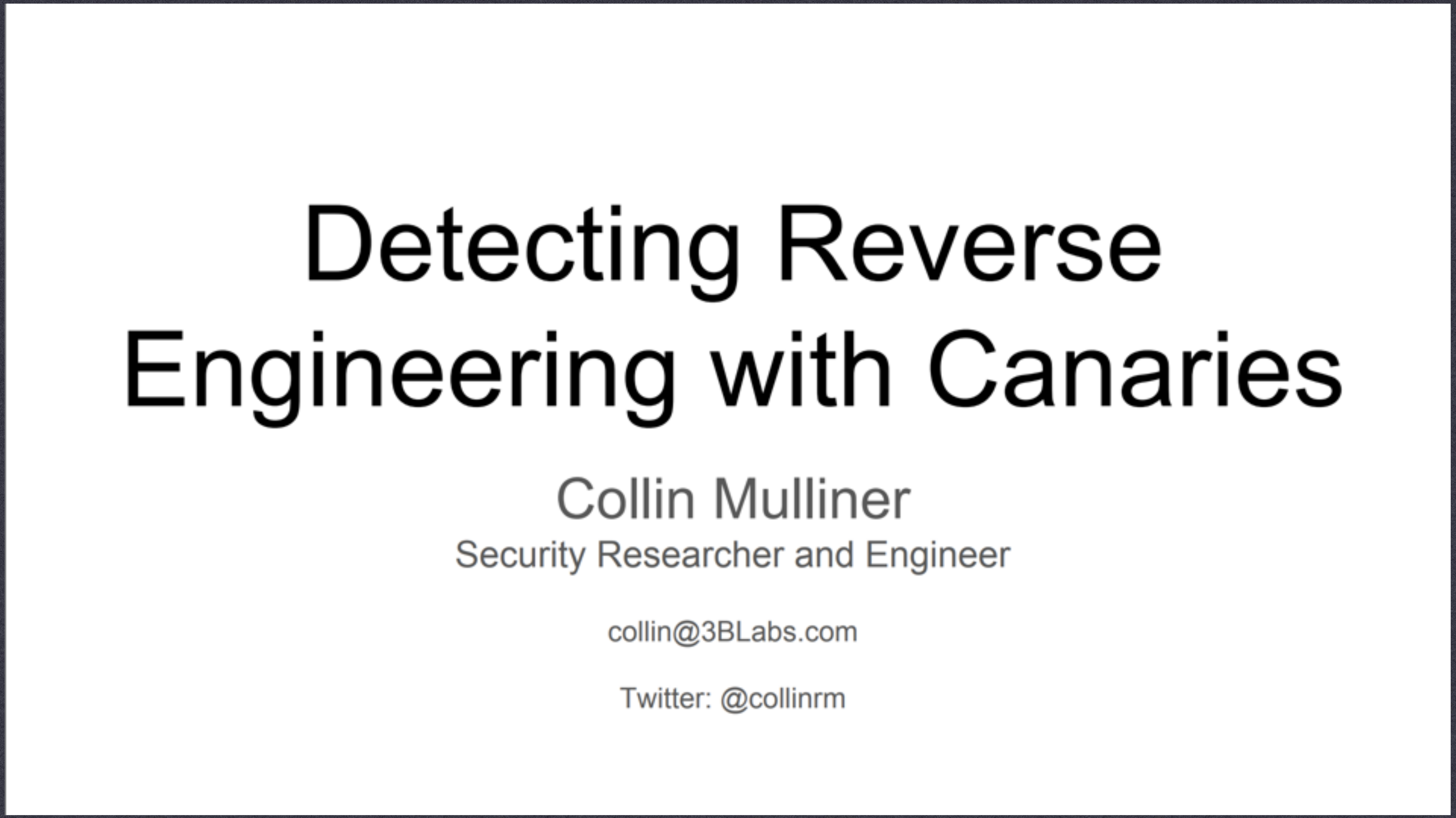
Canarytokens by Thinkst

What is this and why should I care?

Select your token
Provide an email address or webhook URL (or both space separated)
Reminder note when this token is triggered.
Fill in the fields above

Brought to you by Thinkst Canary, our insanely easy-to-use honeypot solution that deploys in just four minutes. **Know. When it matters.**

© Thinkst Applied Research 2015–2018



Detecting Reverse Engineering with Canaries

Collin Mulliner
Security Researcher and Engineer

collin@3BLabs.com

Twitter: @collinrm

A NEW HOPE

@haroonmeer

NYU
POLYTECHNIC SCHOOL OF ENGINEERING

M
The Coinbase Engineering Blog
Follow
2

Graham Jenson Follow
DataDevSecOps Ph.D.
Oct 18 · 4 min read

You need more than one AWS account: AWS bastions and assume-role

UBER

Uber Security Follow
Dec 22, 2016 · 5 min read

Engineering Security Through Uber's Custom Email IDS

Dan Borges, incident response engi

Phishing is one of the largest and
security team. It's the great equal
Well executed phishing attacks ca

M
Airbnb Engineering & Data Science
Follow
2
HOME
AI
BACKEND
DATA
INFRASTRUCTURE
NATIVE
WEB
OPEN SOURCE

Applause from Sarah Guo and 217 others

AirbnbEng
Creative engineers and data scientists building a world where you can belong anywhere.
http://airbnb.io
Jan 31 · 6 min read

StreamAlert: Real-time Data Analysis and Alerting

Today we are incredibly ex
StreamAlert, a real-time da
StreamAlert is unique in th
infrastructure deployment

Ryan Huber Follow
Mar 1, 2016 · 5 min read

Distributed Security Alerting

sts

https://www.youtube.com/watch?v=pY4FBGI7bHM

https://www.youtube.com/watch?v=lrGbK6fE7bI

Its all so wide open again..

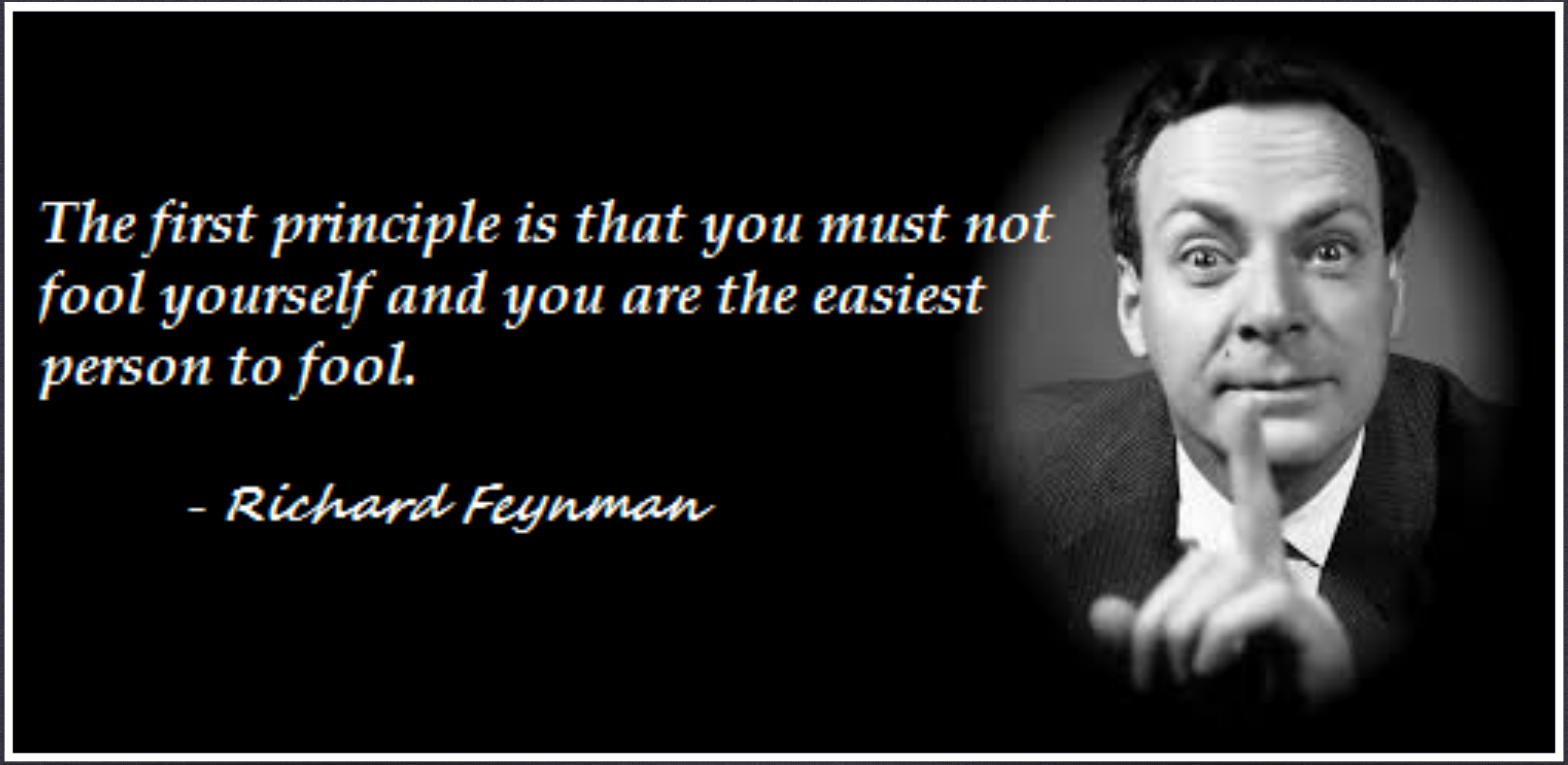
Apache - nginx

wireguard

There are sooooo many cool things to be done..

There are so many important problems to solve…

Don’t waste your time being that other guy..



The first principle is that you must not fool yourself and you are the easiest person to fool.

- Richard Feynman

Questions | Comments | Abuse

@haroonmeer