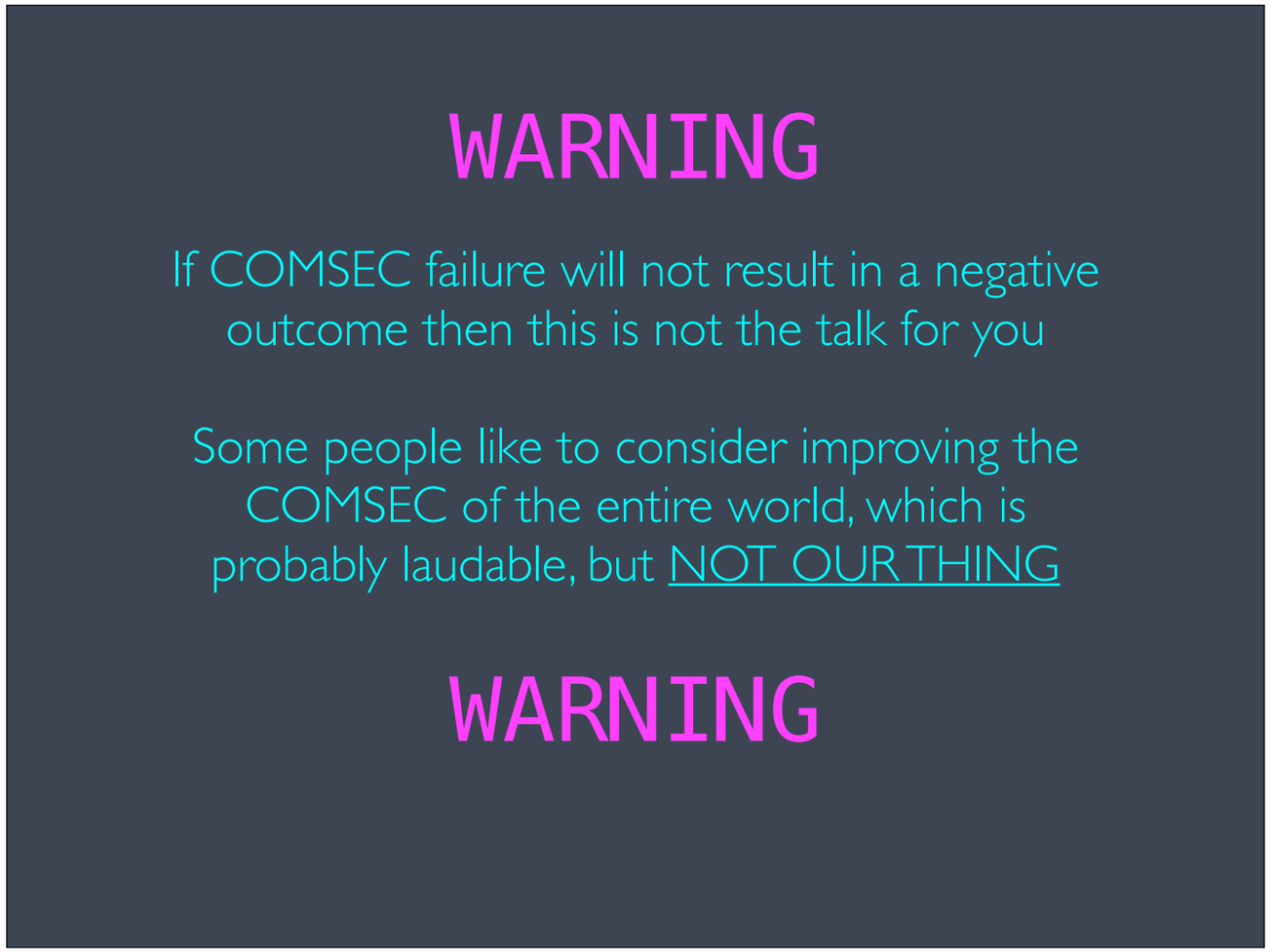

Best title slide ever.

By Ben Nagy (@rantyben) and The Grugq (@thegrugq)

We've added full notes, but you should be aware that they're not all things we actually said during the presentation, these are just some explanatory notes so that we can publish what is, effectively, 101 lolcat slides.




It's a pretty fine line between OPSEC and COMSEC. Everyone is free to practice COMSEC, whether or not they're operational or whether or not they're facing a genuine adversary. However, in that case, it's impossible to construct a threat model ( because there's no threat ), which makes a lot of the tradeoffs moot. The school of thought that holds that all commo failures are the fault of developers for not making things SO usable and pervasive that "average users" cannot ever get things wrong is stupid. It outsources understanding to the developers of those "usable systems" which also outsources trust - but those devs won't be going to be going to jail for you.

The reason we subtitled this talk "Beyond Encryption" is precisely because there are large swathes of COMSEC that having nothing to do with the tools themselves. If you get that stuff wrong, even with the magic super-usable unicorn, you're still going to see the inside of your potential negative outcome. If you get it right, then even total tool failure may not be enough to sink you.

# BEARS

“I dont have to outrun the bear - I just have to outrun you!”

This is the worst analogy ever.

The Bear is LEO. With care and attention we can beat LEO, and we want to be in the woods ( where there are bears ), because the woods are full of heroin money… or honey or whatever metaphor thing everyone wants.

1. None of you can outrun the bear. Bears run at 60kph
2. The first person that gets caught by the bear won’t get eaten. They will snitch.
3. Next, the bear runs you all down, one by one, at 60kph, and kills you
4. The snitch will never do jail time, get a million dollars for their life story, and party at VICE.

So the moral, if anything, is “run slowly and learn to speak bear”

**“People must communicate.
They will make mistakes,
and we will exploit them.”**

–James Clapper, DNI

Spook jargon: “commo" - all comms between targets

# COMMUNICATIONS

Introducing the concept of a “communications event”. We want people to recognise that every CE presents an opportunity for the adversary. Learn to notice CEs. Next, recognise that there are properties of CEs that can help your adversary which have nothing to do with the content of the communication. Did you communicate? Was it on a schedule? With whom? Was it correlated in time or space with another event?

Another thing I want to mention is that, in this image, that note is about to be out of the control of party A and forever in control of party B. If there’s something in that note which could be detrimental to party A then they’ve created a permanent vulnerability. More on that later.

[raw notes]
CEs are natural edges between communicating parties. Bam. Directed Graph.

Several of your potential adversaries are great at analysing graphs. This helps them with:
- constructing hierarchies
- mapping networks
- associations ( adding new nodes )
- (mobile phone) noticing co-travel ( how you failed at COMSEC without COM )


# ANONYMITY

true anonymity is what you want when (and only when) the CONTENT of the CE is the only important thing. Anonymity is when, out of the set of all possible authors, there is an equal chance it could be any one of them. You probably don’t want this for comms within your illicit organisation.

# PSEUDONYMITY

whereas pseudonymity is what you usually want - when reputation matters. We don’t know who is in the suits, but we know that pink snakeskin has come through for us a few times in the past but blue swirly is an asshole.

# MO' MEMBERS, MO' MURPHY

This is now leading into properties of communications systems. According to Grugq's research, the ideal size for a cell is five people. Each person you add increases the chance of a failure that will affect the operation of the entire team.

[raw notes]
A big problem with communication events: they involve at least two people. The more people are involved with an operation, the more likely one of them will be Murphy. Also, even if you are trained and careful in your comms, the other person probably isn't, so you need to ensure they don't screw it up:
"This is Sam, I am calling for David"
"Sam? I don't know any Sam. There is no David here!"
"Sam. Remember Sam? Your friend? From the reception?"
"I don't know any Sam… oh, wait, the KGB guy! Yeah, do you have my money?"

# TOOLING CONCEPTS


so let’s start to think about how we might form a framework in which we can evaluate tools

# CIA

look at this bro. He has the best cover ever. CIA? Are we talking about the agency? No! We're talking about CIA like CISSPs use. He's a CISSP now. Or is he the second assistant regional sales manager for the north west? WHO KNOWS

Ben: "That is the moustache of trust"


# CONFIDENTIALITY

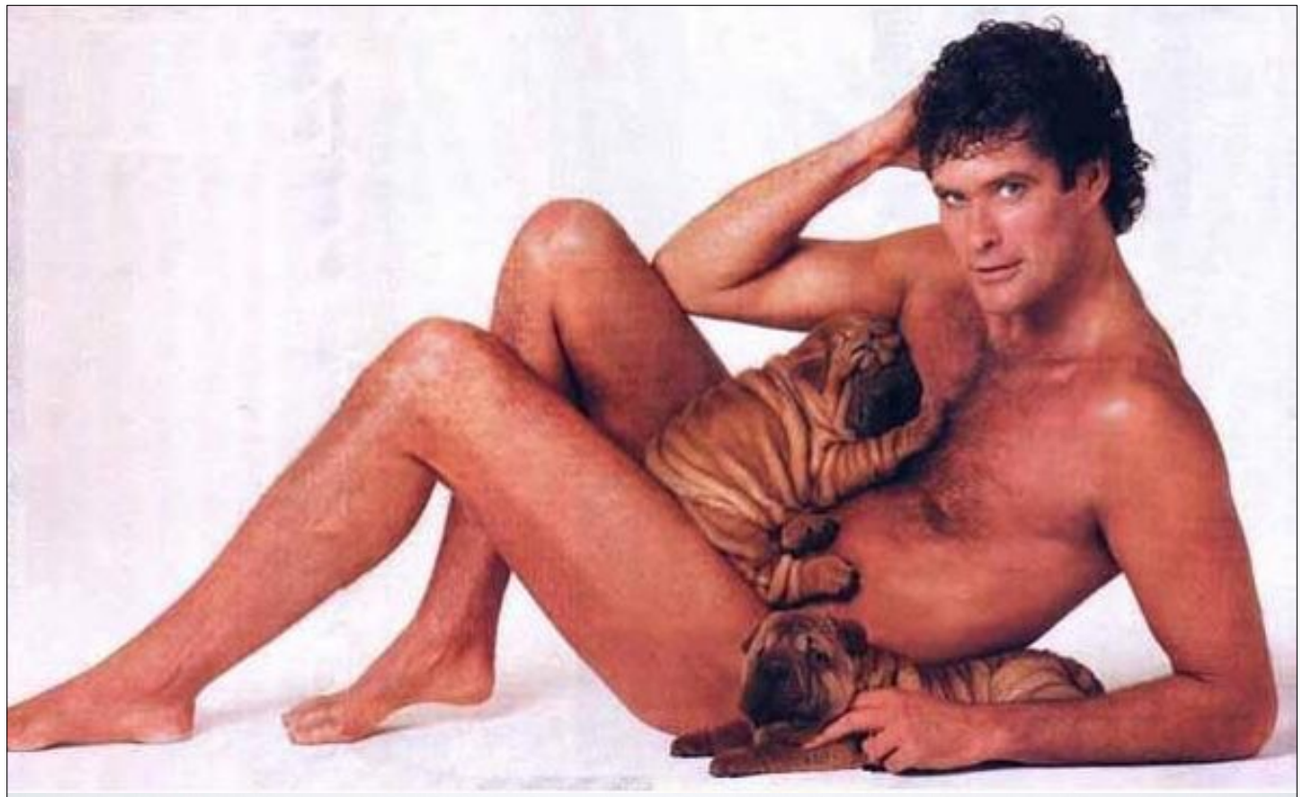
So we’re going to take the old CIA triangle and use it as part of a thought experiment. Confidentiality maps pretty well, but it’s only a tiny part of the picture.

# INTEGRITY

Integrity is the confidence we have that the message is unmodified. Also identity. Both areas overemphasised

People used to obsess about this stuff. How do we KNOW a message is genuine? We want CRYPTOGRAPHIC PROOF. In fact, we want non-repudiable MATHEMATICAL GUARANTEES that this message came, unmodified, from real, live, real-name person X. What we want, in fact, is to provide our adversaries with chains of evidence that are as solid as number theory knows how to make them. Lovely.

As I write this, the prosecution has showed that DPR's private PGP key was on Ross Ulbricht's laptop. How's that strong proof of identity looking now?

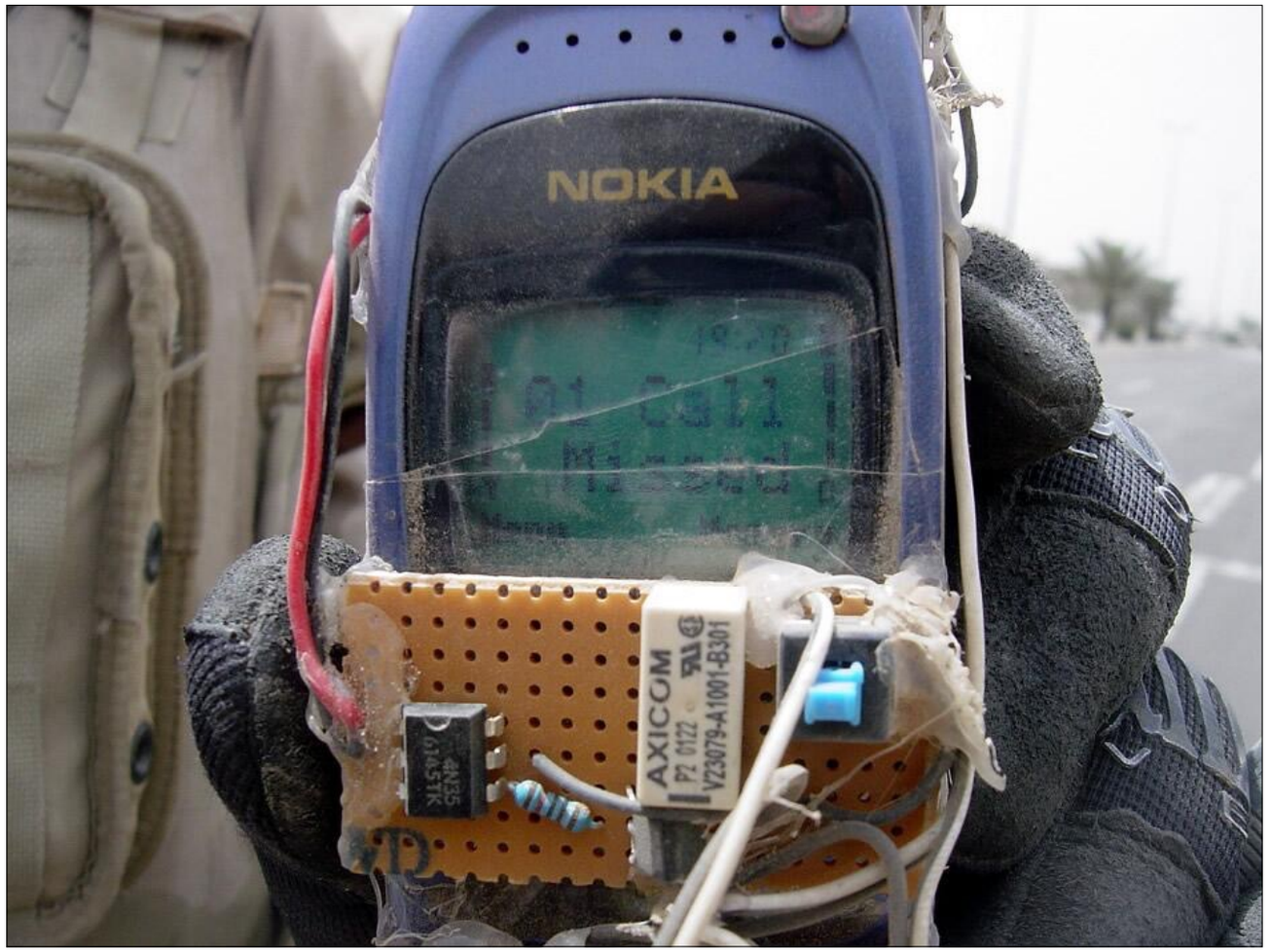


# AVAILABILITY/LATENCY

obviously the perfect image to sum up availability is … not this

Availability doesn't map very well. This CIA thing was my idea and this is definitely a weakness of it, but it's only a thought experiment. What I'm using it for here is more or less "latency". It seems to me like everyone has a huge interest in Instant Messenger tools. It seems to me like all the traffic confirmation attacks against Tor exploit timing correlations. I understand that _sometimes_ you're in a crashing hurry, but you have to remember that CE timing is a channel of information, and so lowering latency automatically increases the bandwidth along that channel - which may well be completely open to your adversary.

Also, SharpeiHoff is the new RickRoll.




of course, sometimes all you need from your system is for the communication to be successful


# C3

cover, concealment, compartmentation

Anyone that has read anything, ever, by Grugq has heard him talk about this. Here we extend our tool analysis experiment to consider the three C's. The CIA stuff above describe properties that are intrinsic to the tools themselves. The C3 factors are more like ways that the tool enables (or handicaps) strong operational processes.

# COVER

ProTip: Islamic terrorists shave their beards when they go operational. If you see a guy in Peshawar buying a razor, run. ;)

This is a CCTV shot of an actual Hezbollah operative on his way to blow up a bus. Does he look like a terrorist? No, he looks like some backpacker schmuck on his gap year.

Cover is your first line of defense, and aims to avoid closer scrutiny. In the presentation we talked about different kinds of cover. For example you could explain that you're in the Cologne Hilton dressed as a clown because you're on your way to perform at a children's birthday party tomorrow in Frankfurt and your flight was cancelled due to snow. That's a cover. There's another kind of cover called "apparent cover" where the observer automatically fills in your cover story in their head - like if you were just wearing a Cologne Hilton chambermaid's uniform.


# CONCEALMENT

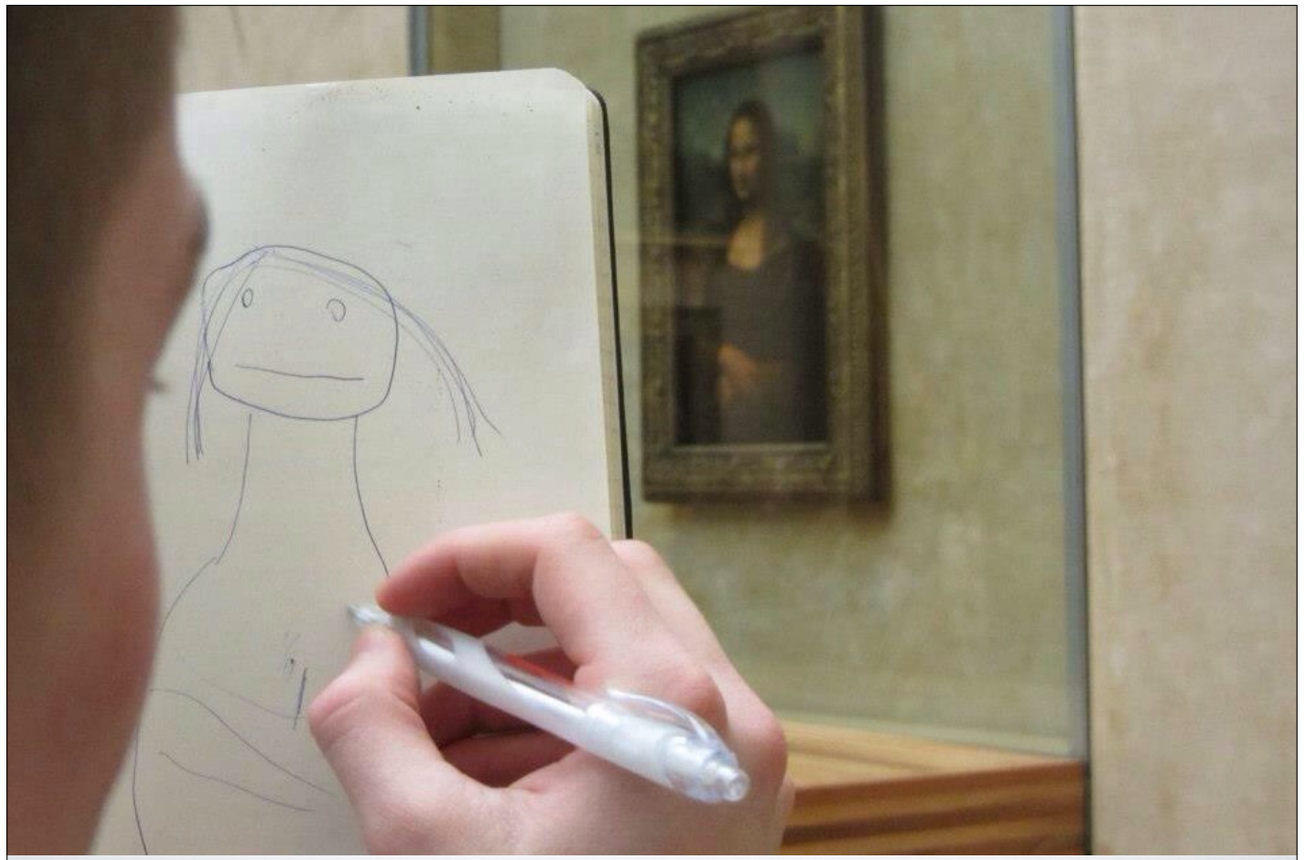
This is a liquor bootlegger's truck. The reason cover is great and concealment is less-great is because at this point you have already started providing either evidence or impetus for further investigation. If I stop you at the border and you have a Blackphone then I may begin to suspect that you may be more than a simple tourist. I may never be able to access your secure device (*COUGH*) but you've already given me a reason to keep an eye on you, and operating under scrutiny is orders of magnitude more fragile.

I wanted to remind people about Eldo Kim here ( the Harvard bomb threat hoax ). He had pretty good Concealment ( was using Tor ) but had no cover to explain WHY he was using Tor at that time, and then gave it up under questioning.

http://grugq.github.io/blog/2013/12/21/in-search-of-opsec-magic-sauce/

# COMPARTMENTATION

Compartmentation is the foundation of good security. When all else fails, your compartments limit the damage. Reduce the amount of sensitive information in any one place, such as a message, or mail spool, or comms device. Things like PFS provide compartmentation in time, reducing the amount of information within a channel.




[raw notes (they are… raw.)]

Tool failure can hurt.

If you're the EFF or PCWorld you have to be "fair" about comparisons and rankings. You're NOT THEM. Don't be fair. It's your neck.

- libpurple. Just…no.
- Writing C is hard. I don't give a shit who wrote it, other factors equal, I'll take a tool in a memory safe language over a tool in C. So unfair!
- "Open Source" as a measure of quality is bullshit. Many eyes don't see squat. It's orthogonal AT BEST to quality ( probably actually negatively correlated )
- "Audited" is bullshit. When? By Whom? For What? An audit says that someone asserted at some point in time that the app RIGHT THEN had XYZ issues. Given that it's almost certainly not that point of time any more and I probably don't personally know and trust those auditors I DON'T CARE
- Browser Based Tooling

Browsers are practically designed to de-anonymise you, and the standards get worse every year. More importantly, it is incredibly difficult to maintain correct DISCIPLINE when sitting in front of a web browser, which leads users to experience COMPARTMENTATION FAIL. In many ways, that aspect of browser-based tools is a more compelling argument against them than all the issues I have with JS based crypto or JS developers.

The ONLY thing that can save you from tool failure is Compartmentation.

# TOOLS

(just cause it fits your need, doesn’t mean you’ll get what you expect)

Let's try some characterisations

GPG Email

A: Slow. No receipt. No guarantees. Bad.
I: No PFS. Very strong Identity if used correctly ( too strong! )
C: A+ would crypto again
Cover: Completely awful. Totally noisy.
Concealment: Utterly terrible. Instantly maps your comms network.
Compartmentation: Horrible. Lost key is total failure, unless you use subkeys or key-per-recipient which is a gigantic pain in the ass
Quality: Medium? In C :( Well scrutinised. Protocol well analyzed


[PRESENTER NOTES CONTINUED]
Tor

A: Fast. Resilient.
I: Traffic routinely MitMed at the exit node, but apart from that, pretty good for HS etc
C: None for first mile, none from the exit to the destination. Only designed to protect traffic from relays themselves and adversaries that are monitoring in-tor links
Cover: Fairly bad. Fingerprintable. No cover traffic ( this is how pretty much EVERY SINGLE HS ATTACK IS ABLE TO WORK )
Concealment: They will know you're using Tor. Apart from that, sender/receiver unlinkability is the one single design goal, so that part is OK.
Compartmentation: Don't have to run on your real box ( PORTAL ), plays well with other compartmentation strategies ( VMs, VPNs ... )
Quality: C code. One implementation, but well funded dev and lots of scrutiny. Good.

AND YET I use GPG as part of my "secure" comms and don't trust Tor, despite Tor appearing to "score" better. Why?

Tor's one weakness is the only thing I would want it for.
PGP's one strength is the only thing I care about.

# NSA PROOF TOOLING

“Dude, look at your skull. You can’t even look up. Plus, you’re a mouse.”

A quick word on NSA proof tooling.

There is no NSA proof tooling in any meaningful sense. There might, in some universe, be an NSA proof combination of incredibly disciplined COMSEC / OPSEC that will work for a finite period of time. Happily, you’re not on their radar, because you’re mouse.

# TELEGRAM

if guys with a PhD IN CRYPO don’t even know what your crypto protocols are defending against, that’s a bad sign. Telegram might not be broken, but it might not be secure either. These statements are equally true… and that is exactly why you should not use it. No one has a clue why it does what it does.

# CRYPTOCAT

So much ambition.
Cryptocat sets out to solve probably the hardest possible problem [multiparty, instant, easy, web delivery]


# SKYPE

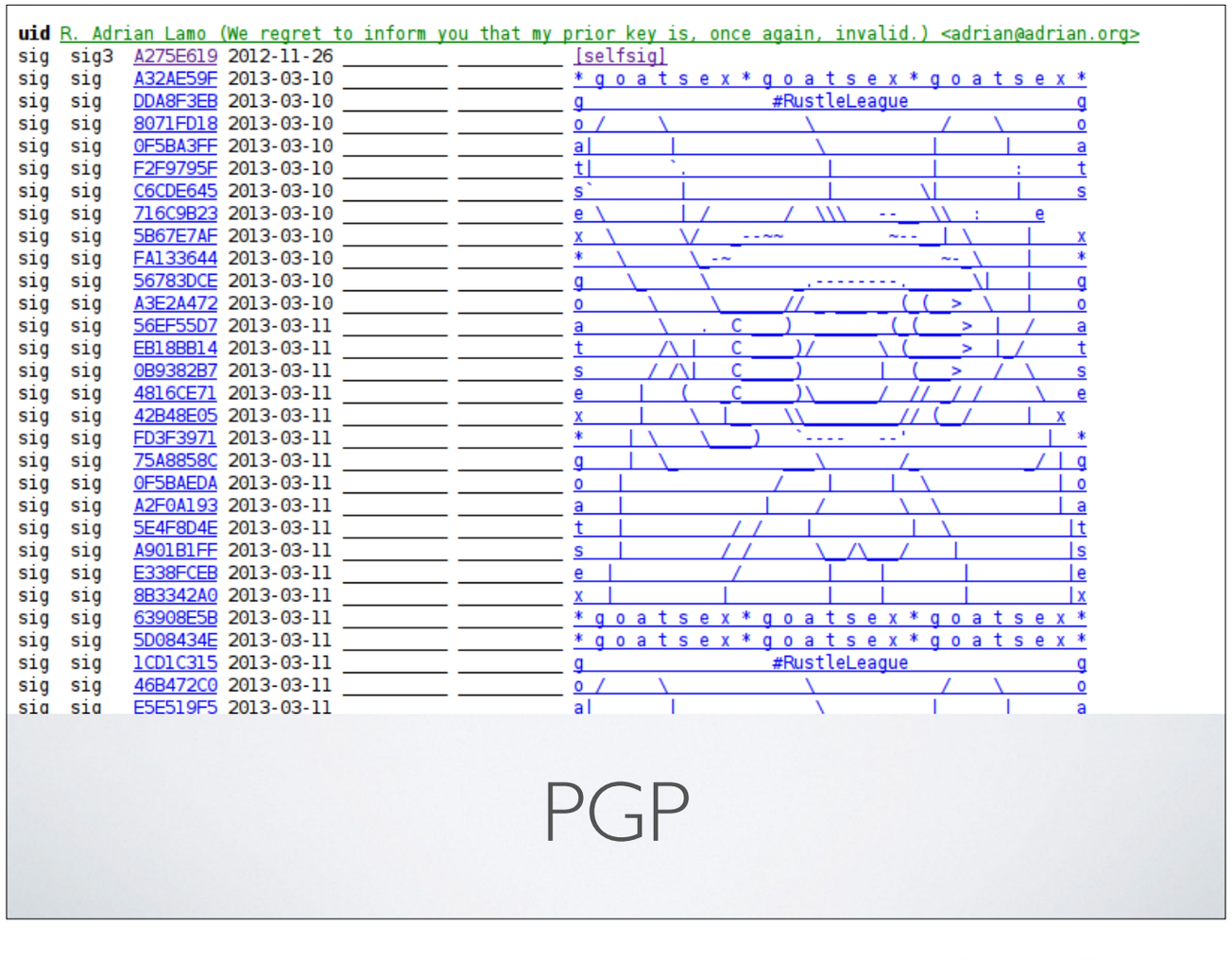
Funny story - rumour was that NSA offered “billions” for the ability to read Skype. Then Microsoft bought it for billions and rearchitected it so that everything goes through centrally controlled servers… and suddenly Skype logs are included in affidavits!

**End to end or GTFO**


rite? Facetime is actually awesome. Great cover, works everywhere, free, secure hardware, end to end encrypted. Provided your adversary can’t legally compel Apple to subvert your keyring… if so, see next slide —>

**“If you are the target of a nation state you’re going to have a bad time. Even if you don’t have a computer.”**

–Matthew Garrett




# PGP

If the Ulbricht trial had been going on when we were preparing this deck then we would have used the Austin Powers “That’s Not Mine, Baby!” scene with the penis enlargement pump. There are some … issues with having a very public record of your PGP key.

Basically everything that PGP guides tell you to do is horrible for your own security.

* Web of trust? More like “provable ring of known co-conspirators and associates”
* Signed message? More like “cryptographic proof that I wrote this incriminating statement”
* Key server? More like “public database of potentially incriminated email addresses”

With PGP remember the mantra: more keys, more often. Generate them more frequently, and stop using them rapidly.


Source: http://www.slate.com/blogs/behold/2014/03/03/_lvaro_laiz_photographs_the_transgender_community_in_mongolia_in_his_series.html

The accurate quote ( line was ad-lib ): “Tor makes you stick out as much as a transgender Mongolian in the desert”

http://geekfeminism.wikia.com/wiki/Kiwicon_2014_expulsion


latency is directly correlated to security. low latency, low sec, hi latency, high sec

There are almost certainly a great many aspects of your OP/COMSEC activities that could be made more resilient by sustaining a little more latency.

Remember: distance in space and time increases security.


Pond is our favourite tool for near-time messaging.
Timing attack resistance, totally untrusted server, EC crypto, Axolotl ratchet, attachments, automatic message deletion, all native in a memory safe language

https://pond.imperialviolet.org/
Threat model: https://pond.imperialviolet.org/threat.html

If you take nothing else from this presentation, take this: compartment more.
But if you take two things from this presentation, also take this: think before you tool up…
And if you stretch to three take aways — just use Pond.

For almost any use case you have, Pond addresses it correctly.


OK so we've had our fun mocking tools. Now let's mock whole operating systems instead.

# THE GIRAFFE OF ASSUMPTION

Some people have formed opinions about platform security that are strongly influenced by either what they WANT to be the case, or by things that were true fifteen years ago but have since changed. This can be their spirit animal.

# LINUX

The level of self-delusion among linux devotees is unusually high. While it is certainly possible to configure, deploy and maintain a very secure Linux environment… ain’t nobody got time for that! The defaults, and the applications, are just not very good.

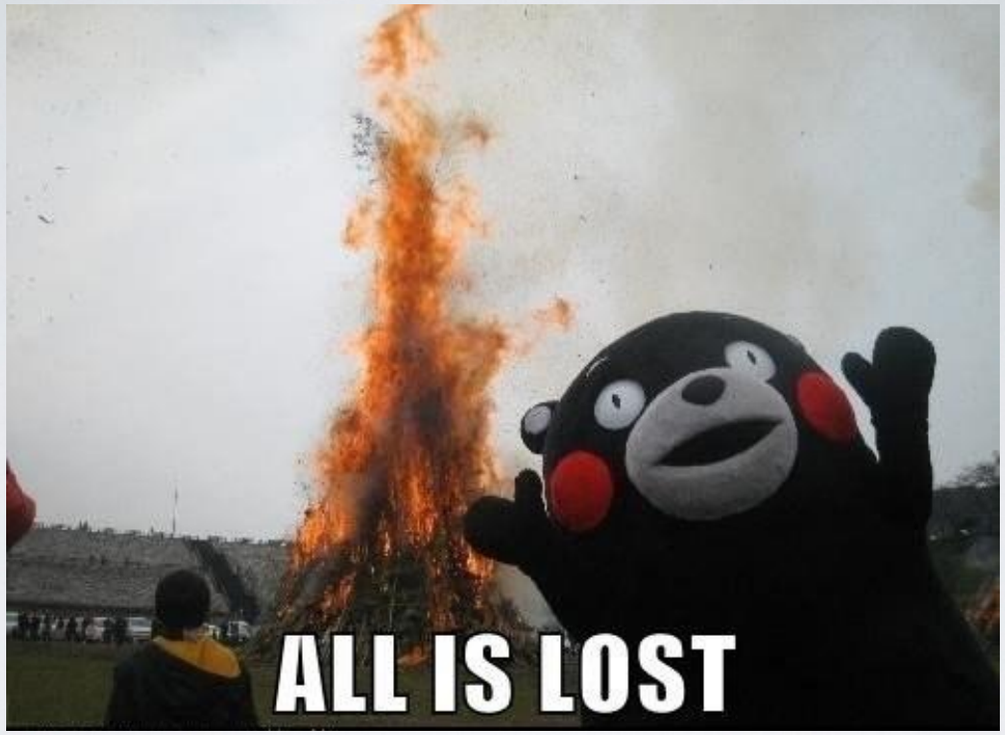

# WINDOWS

Windows is currently the most secure mainstream OS. I mean, we can’t stand _using_ it, but that doesn’t change the facts. The kernel is golden, the userland protections are stellar, and the user experience is somewhere between the 8th and 9th circle of Hell. Not to mention it looks like a lesser Mondrian faithlessly copied by a colorblind monkey.

# IOS

iOS looks cute, but it’s hardcore.

The iOS “walled garden” goes a huge way towards providing what is, in fact, pretty secure platform. Through multiple iterations of kernel improvements and jailbreak defences they’re setting the bar higher every version. As with Windows, some people formed opinions based on versions from several years ago and never readjusted them.




# ANDROID

All the security of Linux … plus Java! “Java: The malware compatibility layer of choice”

Android can be engineered for security, but when you’re done you have a hermetically sealed self contained comms device — not a smartphone.

**“We stopped using mobile phones. When we use them, we die.”**

–Taliban commander

You can't communicate securely with your mobile phone. Nor with a burner phone. Nor with someone else's phone. Not with any mobile phone in any situation ever. Don't use mobile phones.

"That's unrealistic advice!"

[ben] I haven’t owned a mobile for over a year. Not for security reasons, just because I wanted to see if I’d drop dead or my arms would fall off or something. They didn’t. This leads me to believe that if my threat model included negative outcomes such as death, torture or life in prison then I would suddenly become able to follow this “unrealistic” advice.

[grugq] for the record, Ben lives on an island with 2 bars, if the person he wants to meet isn’t in one bar, they’re in the other. #justsaying

# FINAL THOUGHTS

We all know that what's really going to happen is that everyone will latch onto the tooling section, and compress the whole presentation to "Pond COMSEC Good!". This is actually the exact opposite of the point we were trying to make, but it's inevitable. Nonetheless, here are the takeaways we WANTED to leave people with…


Blurring the OPSEC / COMSEC line here, again, but it’s very important to realise that COMSEC is not a sometimes food. Assess yourself. Try to understand where you’re weak and strong with operational discipline. When do you get distracted? Where do you make the most mistakes? Can you build your systems in ways that tolerate some error?

"The thing is, you only got to fuck up once. Be a little slow, be a little late, just once. And how you ain't never gonna be slow, never be late? You can't plan for no shit like this, man. It's life.” ~ Avon Barksdale ( The Wire )

# COMPARTMENTATION

Once again, practice compartmentation. Once you accept the inevitability of failure then the only possible way to look at security ( of any kind ) is probabilities and damage control.

# IF IT'S NOT END TO END, IT'S CRAP

An easy way to weed out COMSEC snakeoil is to look for the telltale signs of missing end-to-end encryption.

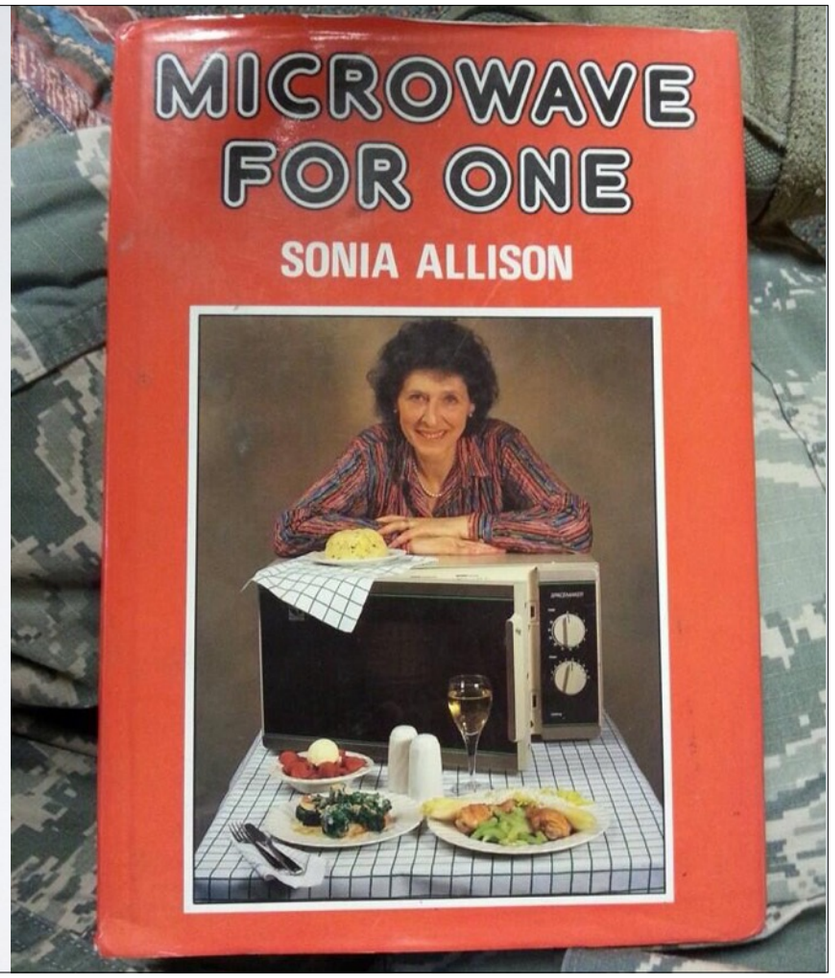
AS ONE EXAMPLE Check https://slack.com/security

- Uses TLS ( so probably user to server )
- "We place strict controls over our employees' access to internal data and are committed to ensuring that your data is never seen by anyone who should not see it." this is called "Lookaside Security"
- "There are limited circumstances when we ever share customer content without first obtaining permission" yeah, bye

# COMPARTMENTATION

Did we mention?

TRUST
NO ONE




[grugq] that is, officially, the loneliest cookbook ever.

If you spend some time reading affidavits and transcripts from successful prosecutions of “cybercriminals” you’ll start to notice a common theme. Here’s a hint - remember the bear analogy from the start?

# COMPARTMENTATION

Many of which would not have been possible if they'd had better compartmentation

# YOU CAN'T WIN


Plan for failure! Professional criminals accept the inevitability of jail, so they plan worst-case in their operations to limit who will go to jail and for how long. Whatever your expected negative outcome you should accept that it will occur. If you can't then you shouldn't be doing what you're doing.

# COMPARTMENTATION

And this is a good way to limit that


The most important message we have to impart is that thinking about COMSEC tools is putting the cart before the horse. Like.. you don’t even have a horse. You just have a cart and maybe you were planning to get a horse next autumn at the county fair. Think about what you’re doing. Be careful. Be disciplined. Plan. Compartment. Avoid blind trust. Know what you want from your tools and then find tools that fit, not the other way around.

Read about other people’s failures. Read court cases, see where the errors were made. Read about unsuccessful prosecutions. How did they dodge the bullet?

Also, I still can’t get over how awesome this image is. It’s even in Kiwicon colours.

# QUESTIONS?

Don’t forget: think, compartment more… and just use Pond!

# THANK YOU

@rantyben
@thegrugq

Now you are the comsec master

BONUS MATERIAL BELOW

“We are not here to fuck spiders” ~ Barnaby Jack

an actual KGB secure phone…

Concealment


Cover


Concealment

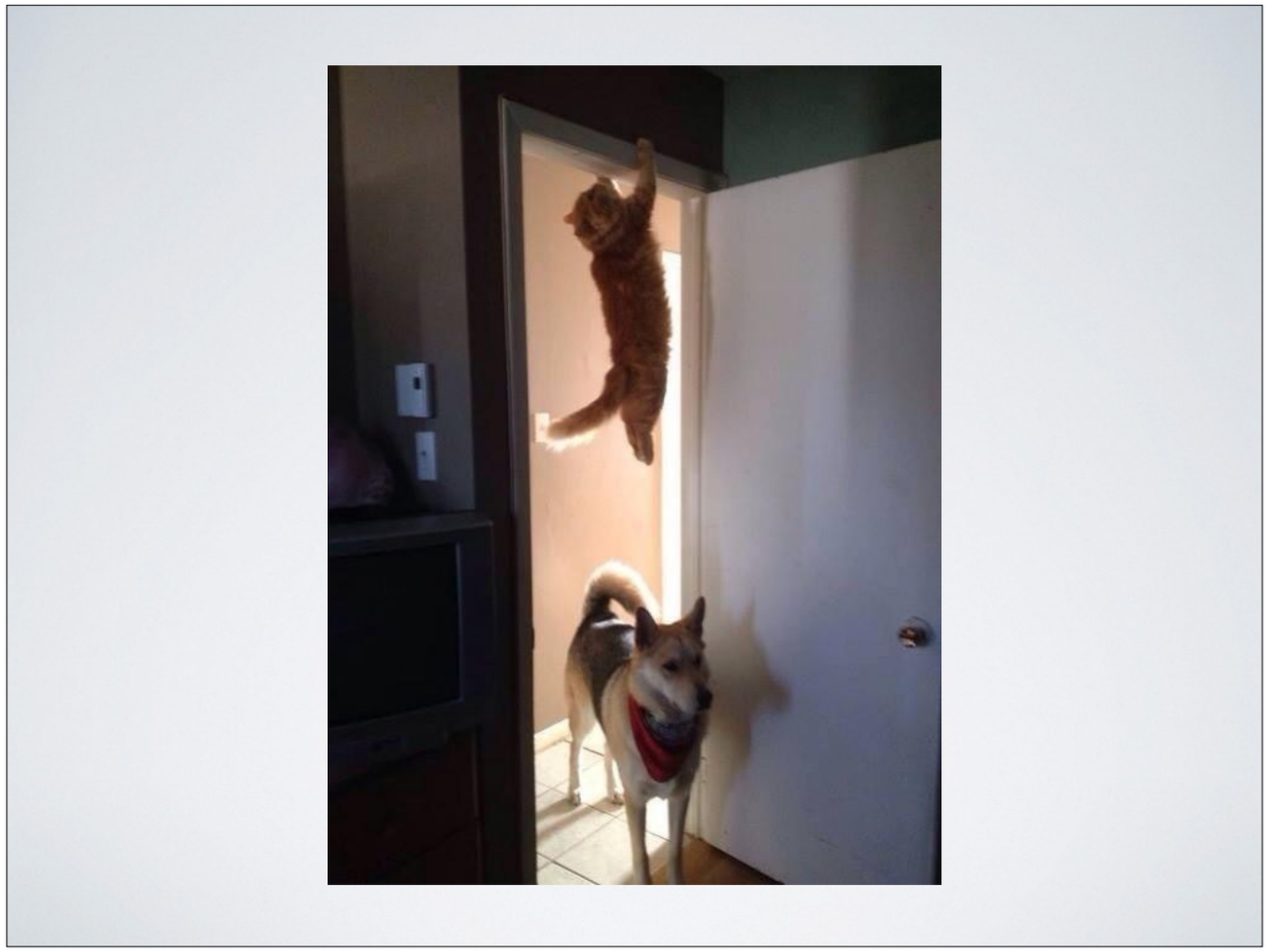

PAYASOS
VILLANOS
LATIN LOVER
REY MISTERIO JR
PERRY ESTRADA
HEAVY METAL
PSICOSIS
HIJO DEL PERRO
JUVENTUD G

I can’t even

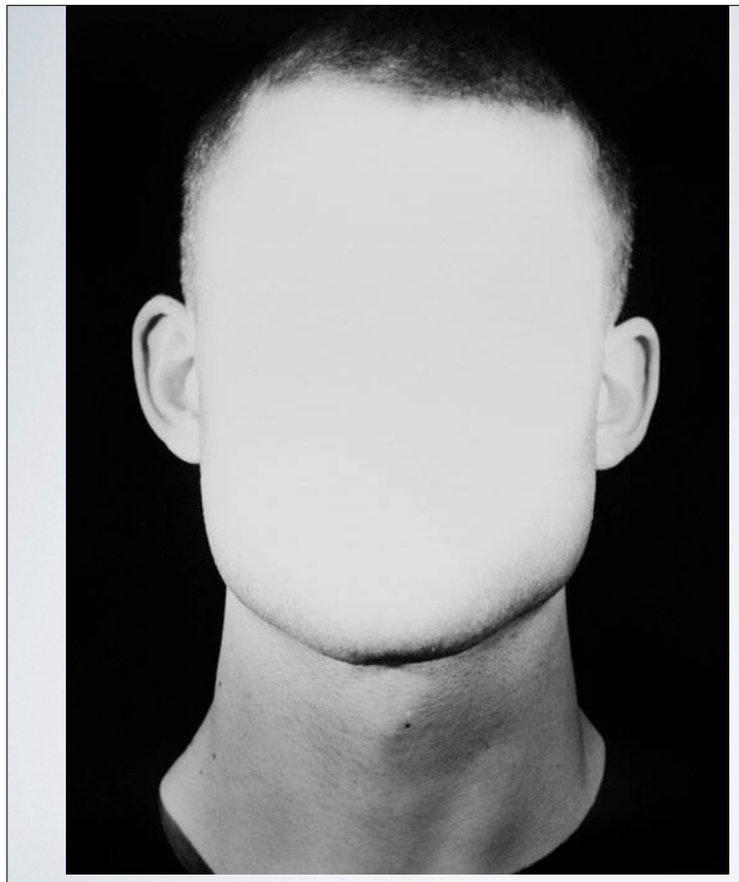
# LOOK ASIDE SECURITY

popping calc on boxes (credit to @aloria)

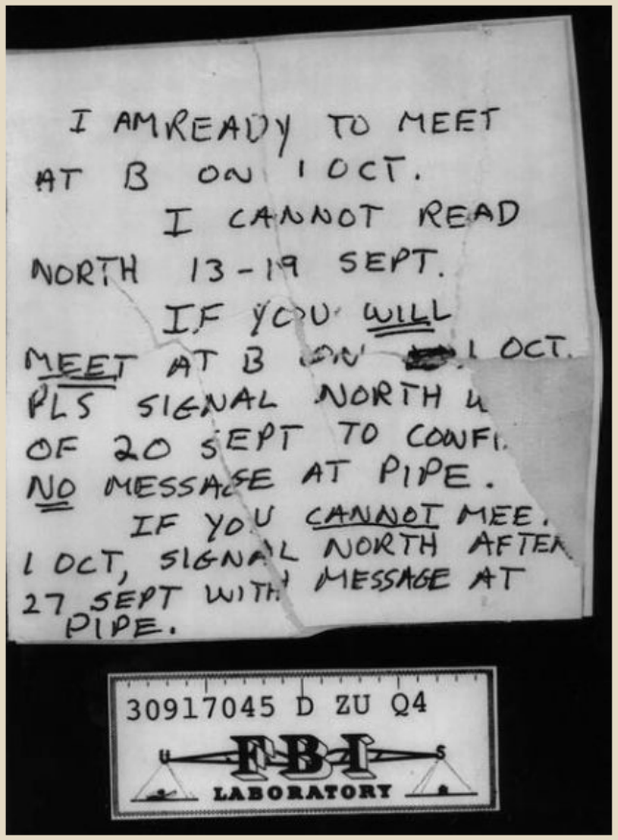

[grugq] I love this. No idea how to fit it into anything… but just look at it!



Understand your adversary’s investigation procedures and weaknesses



something something anonymous…




A torn September 15, 1993, note from Ames to the KGB recovered

This is a great use of Shared Context. “I am ready to meet at B” - by not transmitting information that is known only to the sender / receiver you get both security and also some level of identity confirmation.

One of the things we didn’t talk about enough is minimising information transmitted during communications. The less said, the safer it is. One excellent example of this is using shared context (related: aesopian language) to keep information out of the comms channel. You say “See you at the place at the usual time” rather than “see you at the Wok Inn on Main St at 8pm”


Never go there.

Some tools require training to use.

[grugq] this was going to be the PGP slide… it seems like a great and useful tool, but first time users commit face palm mistakes with alarming frequency.


GEORGE
ORWELL
1903-1950
NOVELIST
& POLITICAL
ESSAYIST
LIVED HERE

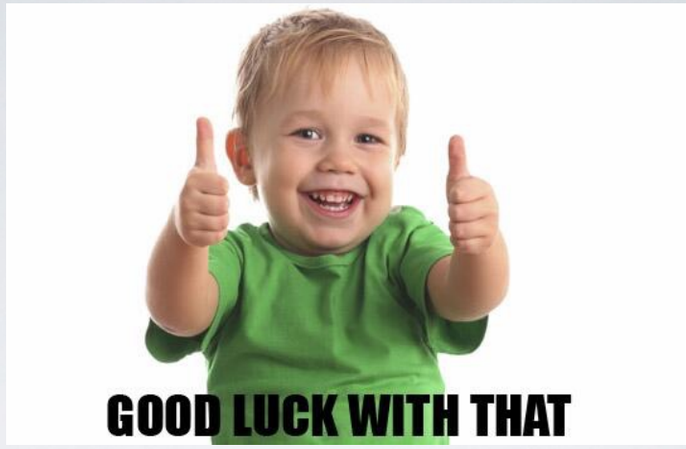
local security forces.

OPSEC 101: STFU


uh...


IF YOU TALK
TOO MUCH
THIS MAN
MAY DIE!

“There is no such thing as tiger self-defence. You can’t just ‘train harder!’ and fight tigers one day.”


GOOD LUCK WITH THAT

Suddenly LEO.

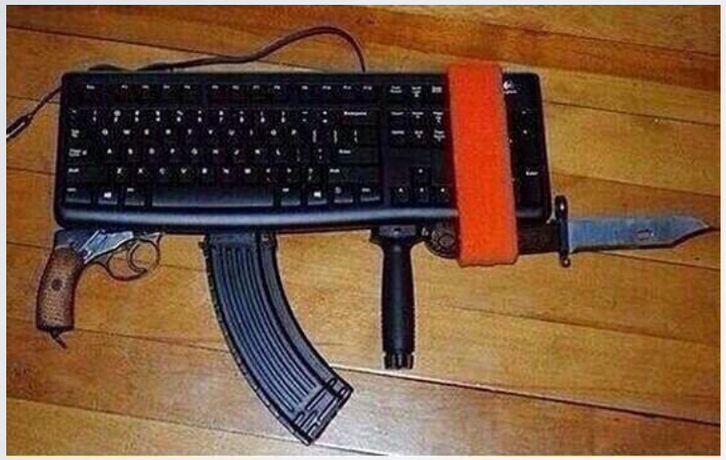
The enemy invariably attacks on two occasions:
1. when he is ready
2. when you are not


crypto tools are generally not safe for users.

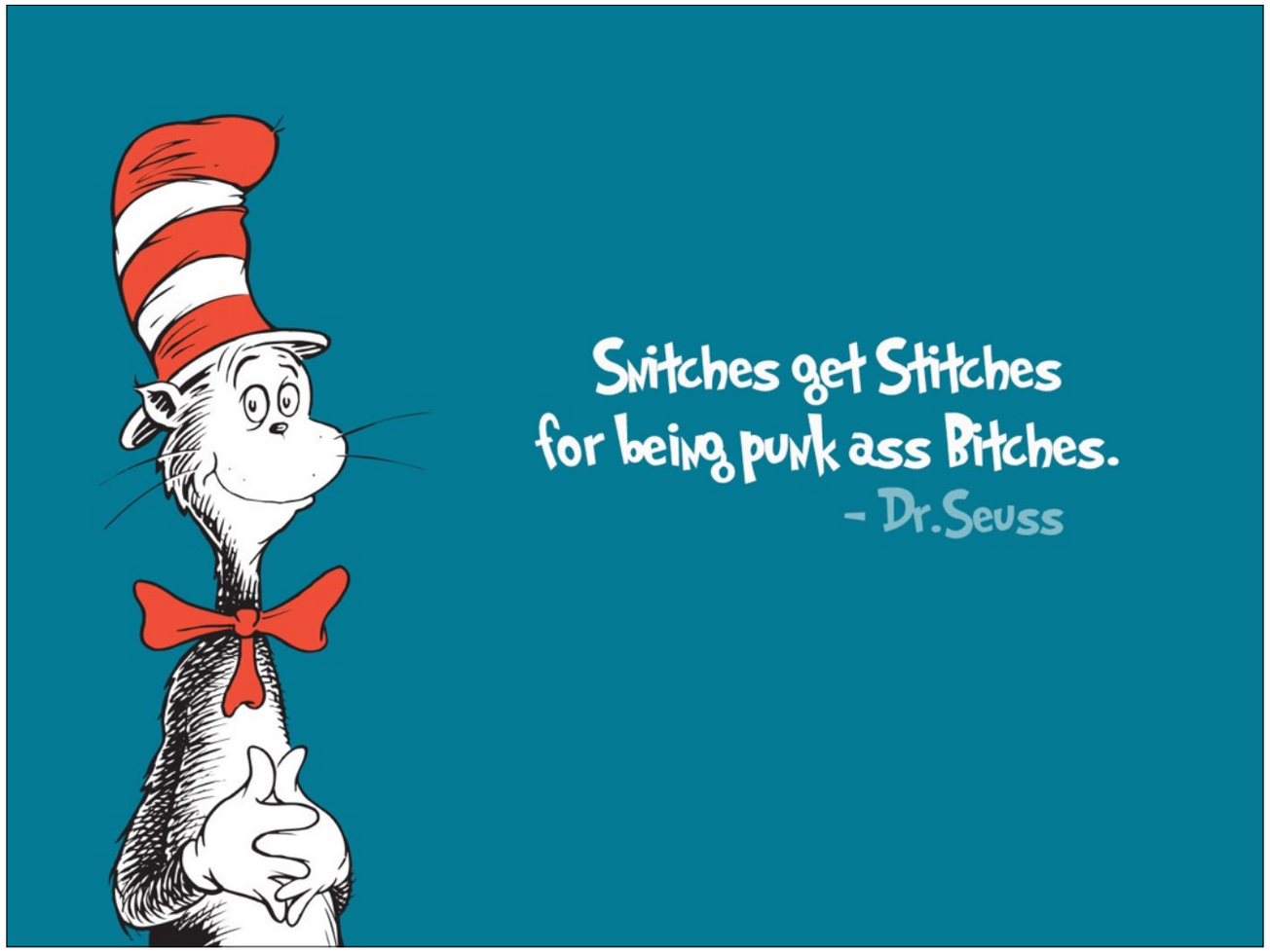
Made sense at the time


Sheep. Because Kiwicon. In New Zealand. And sheep.

Yes, yes, that’s why we didn’t run it.



Cyberweapon



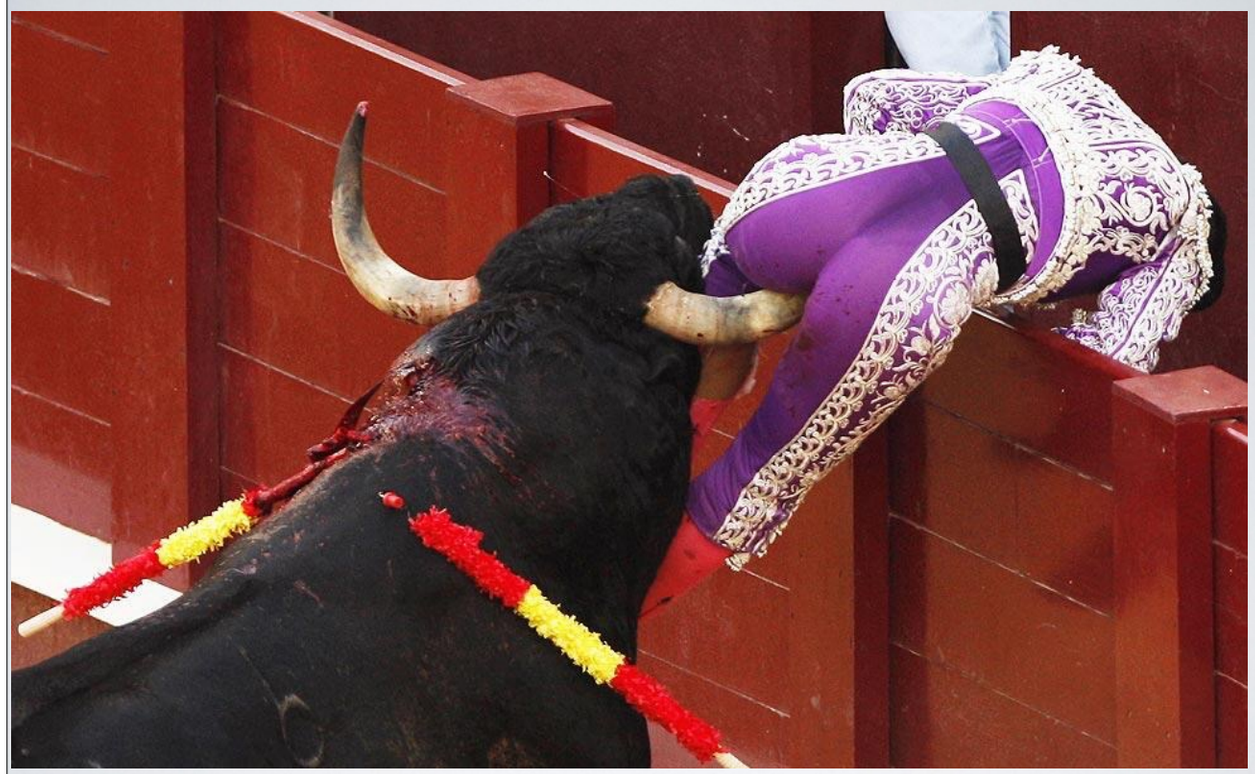

actually, snitches get reduced sentences… only communities and organisations with strong rules against defecting are able to punish “snitches”. See: criminal groups, terrorist organisations, intelligence agencies, etc. Your group of hacker friends, and your hacktivist collective? Yeah, nah. See: Sabu.

100% secure against ebola! What could possibly go wrong!


um… its the gpg UI for handling pgp smartcards with subkeys for signing!


No relevance whatsoever. But funny.

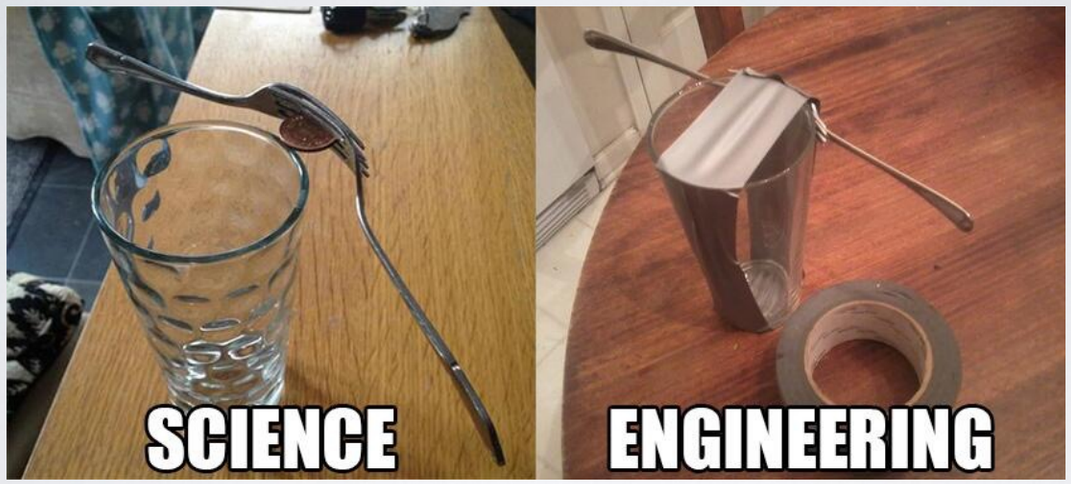
“Tony? They got Tony?? Don’t worry man, I’ll protect you inside!”

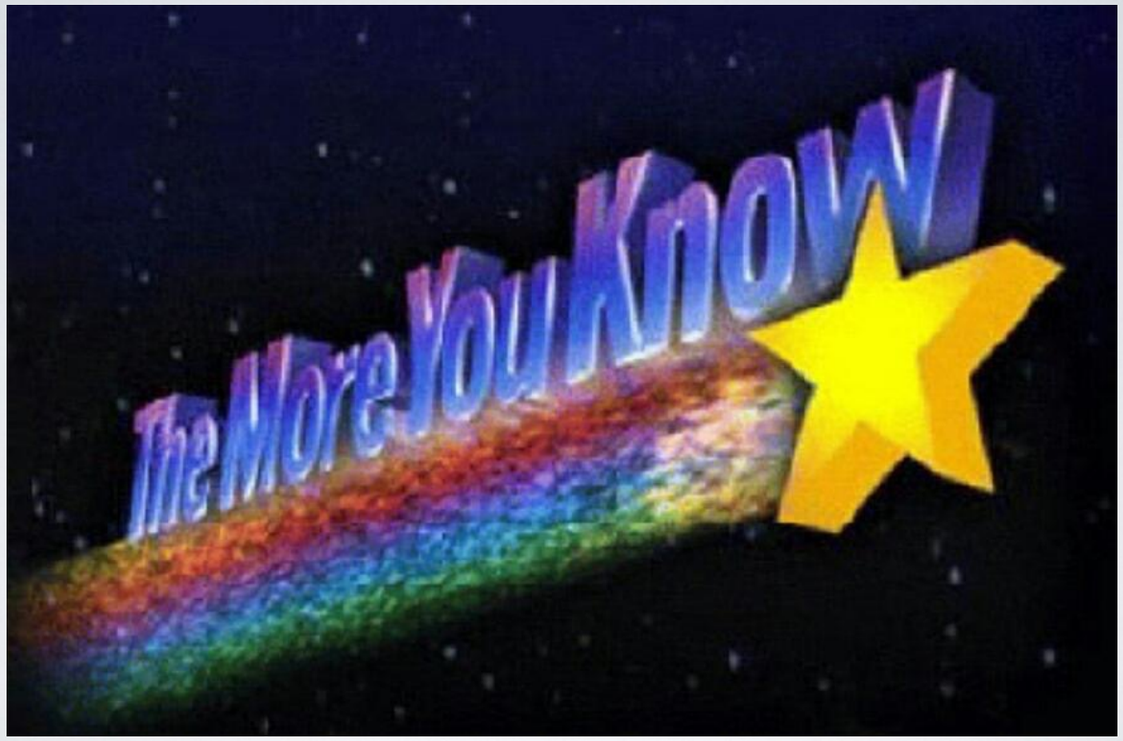


Perhaps best not to irritate certain adversaries

Defence in Depth Failure or something

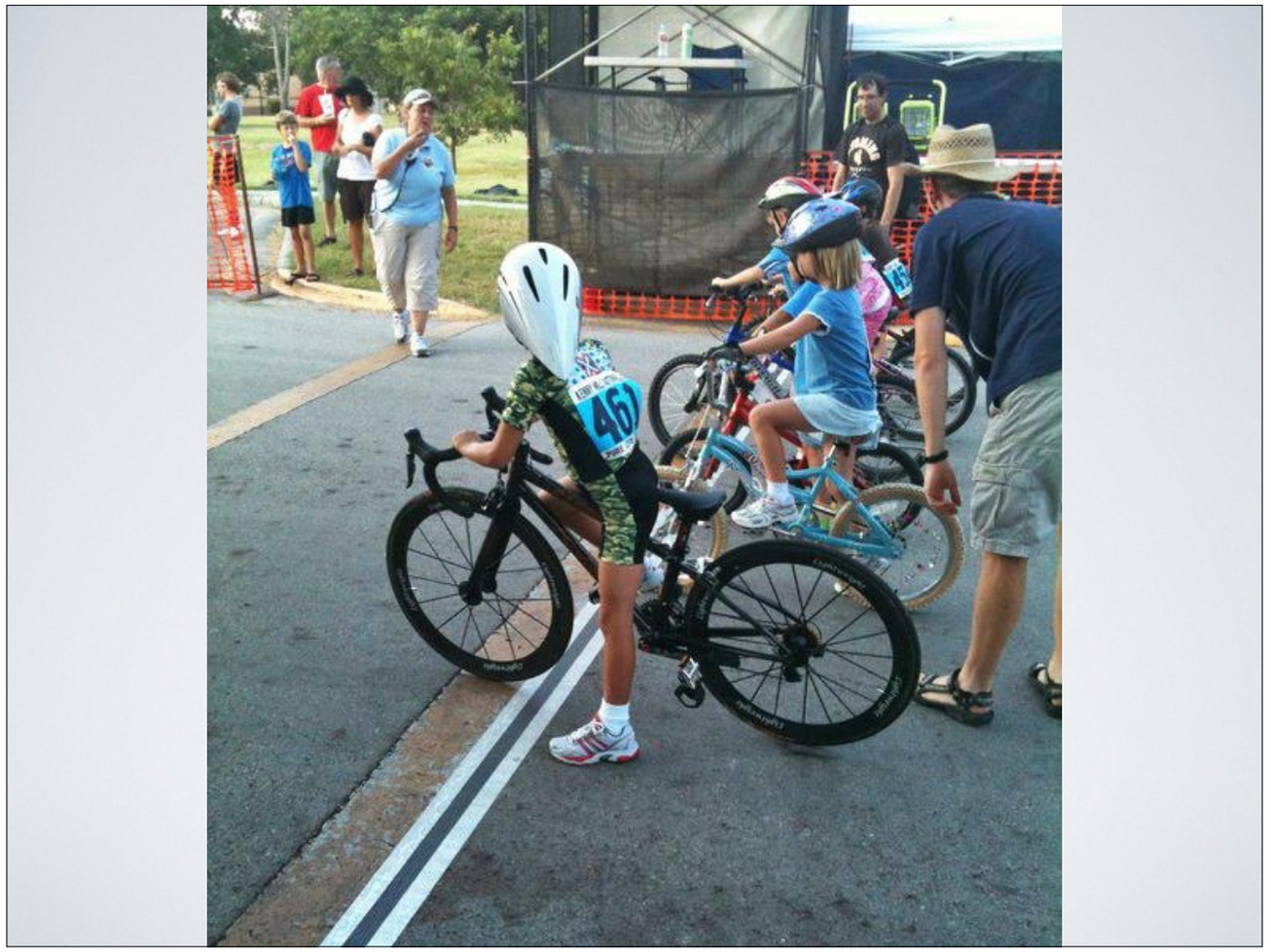

Usable interface.


SCIENCE
ENGINEERING

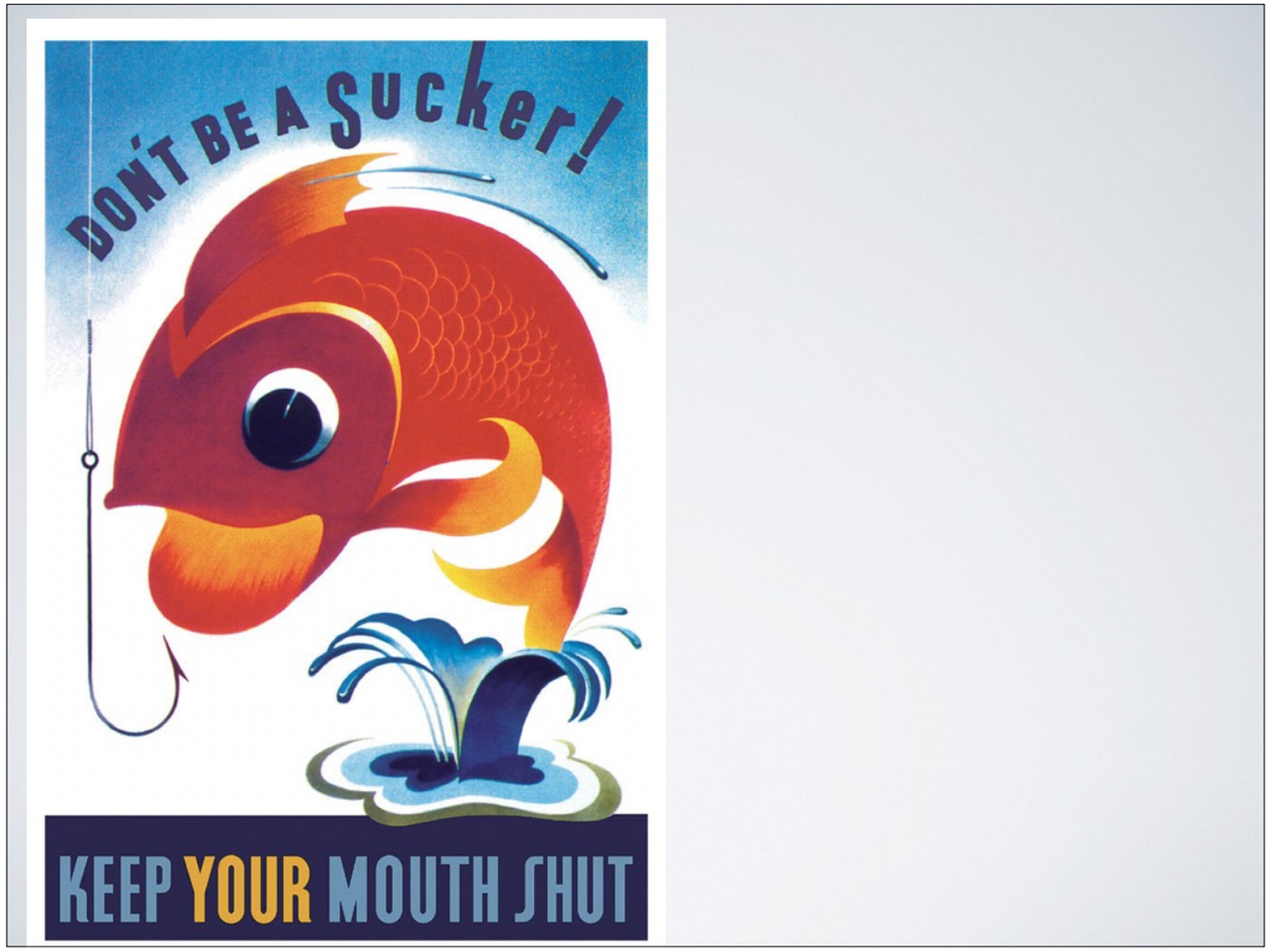

The More You Know

Some tools will not do what they say they will do

mauled in 3.. 2… 1..




It’s the cheating at the start line that really makes it




OPSEC 101