Twitter Thread by foone

foone
@Foone

time to get back to "repairing" old computers

The funny thing about making the 8-bit-guy into a meme about "repairing" computers with powertools is that the obvious heightening joke would, like, the "8 rounds guy", who fixes computers with firearms

but that would also be him, given that he's also a big gun enthusiast.

so it's inherently hard to satirize the repairing-computers-with-dremels guy, since they're also the guns-guy.

you'd have to go up to like a mythbusters level of overkill.

"this hard drive from 1986 won't spin up. We tried freezing it, tapping it with a rubber hammer, and opening the case to lower the friction... there's only one option left: GET OUT THE C4 EXPLOSIVES!"

to be honest I'd actually like to see a mythbusters-style approach to hard drive destruction techniques. That'd be on new drives though, not rare IBM prototypes

things like "can you erase them with a bulk eraser?" (I'm pretty sure the answer is no)
"what if you crush the case?" (probably still resuable if you don't bend the platters, since you could swap the case+PCB in a cleanroom

all the way up to things like how the US military uses thermite.

you could also test that endlessly repeated but never really demonstrated idea that you could take a drive written with data and overwritten with a static pattern, then put it under a precise instrument and get an analog value out, recovering the erased data

the idea there is that magnetization is inherently an analog process, and writing a "1" doesn't result in the same analog value all the time: it depends on what the previous value was

like, to oversimplify:
if you have magnetic material which is in some range of 0-100% magnetized, it starts at 50%
You write at 0, it goes down to 10%
if you instead wrote a 1, it would go up to 90%

but if you then erase it by writing 0s, the 0 will stay around 10%, maybe going down to 5%
but the 1 will only be pushed down to like 20%, as it doesn't fully overcome the previous magnetization

and the hard drive head is designed to amplify magnetic flux differences and convert this to binary, so 5%, 10%, 20%? it doesn't care, those are all zeroes.

but in theory, you could use a more sensitive device to read off the magnetic flux, and tell the difference between a 5% and a 20%, mean you could look at a drive that had been overwritten by zeroes and go "this 0 used to be a 1, and that 0 used to be a 0"

the thing is, although this has been theorized many times, and possibly proof-of-concepted in very limited artificial tests, I wasn't able to find any evidence that it's actually been done.

There are standards for data erasure that take this possibility into account, though. Most of them require either writing 0s then 1s then a static pattern, or patterns that invert, or completely random patterns

which basically just says that "the intelligence agencies who might have enough money to perform this kind of shit suspect that the other side(s) might be able to do it"

and maybe we're just being overly cautious and it's not actually possible, or not possible for remotely reasonable amounts of money.

like if it turns out this is so complicated and hard that we're talking like millions of dollars per kilobyte recovered, it's PROBABLY not gonna ever really be worth it.

anyway, I'd love to see that demonstrated or at least some parameters put on what it would take to be possible.
like "if we had magnetoscopes that were 10x more sensitive and could cool down the drive to within a couple degrees of absolute zero, maybe?"

another destruction method I'd like to see tested:
the platter-drilling method.

because I've seen this argued to be a "complete" destruction method even though you technically only damage one part of the disk, because of how hard drive heads have to float over the platter: a hole in them fucks up the airflow and you'd headcrash horribly.

but it seems like that's really only a limitation in how a drive works NORMALLY.
With some clever hacking of the firmware/hardware, you could possible have a hard drive which has been been

programmed to avoid the tracks affected by the hole

then you could extract the data from the tracks before it, then from the tracks after it

possibly even the track itself, if you can avoid the hole by spinning the drive slower.

spinning the drive slower is going to fuck up SO MUCH decoding code you have no idea.

but it's theoretically possible.

and it's the kind of thing that if, like, the US knew that the KGB was destroying drives by only drilling a hole in them, they might spend the money to get Western Digital to write them a custom modified firmware to handle it

you might want to spin the drive slower anyway: hard drives spin pretty fucking fast, and it's now going to be unbalanced by the hole in it.
it might vibrate itself to death.

anyway, intelligence agencies tend to suggest (and use) very overkill destruction methods, for a couple reasons.

1. they don't want to be surprised by the secret technological abilities of enemies

if you THINK you're fully erasing drives but it turns out they're not fully erased, you really don't want to find that out after 10 years and it turns out the French have been secretly reading all your "blank" hard drives. Whoops.

Like, the Nazis during WW2 knew that Enigma had been broken, they just didn't realize HOW broken it was.
They also thought the much more complicated & secure Lorenz machines were were not decipherable... they were wrong.

And the other reason you want to go overkill is because of capability double-bluffing.
If you are like "We erase all our drives by writing them with zeros" and then one day are like "UPDATE: MAKE SURE YOU WRITE ZEROS THEN ONES THEN RANDOM CHARACTERS..."

The enemy is probably going to rightly assume this means you just figured out how to extract data from a hard drive that had been overwritten by zeros.

By going overboard about your security methods, you keep them guessing about your capabilities.

Which is definitely a thing that happens. Intelligence agencies spend lots of money and time on things that aren't known publicly. Just ask IBM!

in the 70s IBM designed the Data Encryption Standard, DES.
It's a 56-bit cipher, and was an important advance in publicly-available cryptography.
But they published an early version in 1975, then later updated it after talking with the NSA.

And it turns out the original version was weak against differential cryptanalysis. Differential cryptanalysis wasn't "discovered" until the late 80s.

But clearly (and IBM has admitted this now), the NSA knew about it in the mid-70s, and worked with IBM to harden DES, and also do so in a way that wouldn't reveal that differential cryptanalysis existed and in was use.

Because the NSA was in that standard secrecy double-bind:

They don't want to reveal this technique (because then the enemy will harden their systems against it) but at the same time, they don't want their domestic systems to be vulnerable to it

The same sort of double-bind is gonna happen whenever they discover an exploit in a widely used system.
Let's say the NSA figures out how to hack into every linux machine...

Do they immediately announce this and get it fixed so that russian hackers won't be able to crash all the linux machines in the US?

or do they go and hack all the linux machines in russia?

They gotta make that choice. And presumably it comes down to a lot of analysis on how much they can do with the exploit, vs the possible damage, vs how close they think external hackers (white or black hat) might be

by the way, this came up with the original Enigma!
The work the UK did to so completely hack the Engima machine was kept secret for decades

and the reason was that enigma machine was available commercially prior to the war, and many other governments had taken it up too, using a more secure extra-rotors system.

And if the UK kept it secret that they could easily hack Enigmas, even ones with more rotors... they could decode all those communications.

This is why if you look up a computing history book from 1960 it'll be like "The first computer was the ENIAC, built in 1945 at the University of Pennsylvania!"

The Colossus Mark 1 (1943) and Colossus Mark 2 (1944) being still completely secret.

Although the ENIAC can still be regarded as the "first computer", it just depends which restrictions you put on what counts as a "real computer".

like Wikipedia says it was the "first programmable, electronic, general-purpose digital computer"

because there were computers before it that weren't programmable, or weren't electronic, or weren't general-purpose, or weren't digital.

Like you can argue that the Antikythera mechanism is a computer (just a non-programmable, non-electronic, non-general-purpose, non-digital) one, and that's from 200-87 BC.

The other fun side of keeping your hacks secret is the plausible-deniability part.
Like, if every time the Nazis sent out a submarine, a British destroyer sailed directly to it and sank it, they'd start to get suspicious about the security of their codes

So the allies did a lot of work to ensure there were reasonable alternate explanations for why they were "just happening" to stumble upon things they only knew about because Lorenz & Enigma were cracked.

(The Bobby Shaftoe part of Neal Stephenson's Cryptonomicon is all about this)

They also had double-agents whose entire job was to provide almost-useful information.

Because during WW2, every single Nazi agent operating in the UK was discovered, and most were now working as double-agents providing incorrect information to the Nazis.

This was called the "Double-Cross System", run by MI5.

But they didn't just send back incorrect information. The Nazis would figure it out pretty quick if all their spies were constantly telling them "The Allies are gonna invade! They're calling it D-day, and it's gonna land in Pas-de-Calais, on the 12th of June!"

Enough obviously wrong information and you realize your spies are either useless or actively working against you.

So they had them transmitting a lot of accurate information but too late, or almost accurate information... with other information being intercepted to explain why it wasn't accurate.

Things like "The allies are going to sweep Quadrant B-7 for uboats, tomorrow at 3pm" but ensuring the message can't arrive until 2:57pm or even 3:16pm, when the allies are already doing exactly that.

so the nazis would be like "Damn! we were too late.
But man, this spy is great. Let's give them a medal, and tell them to try to be a bit faster with the radio messages next time..."

or sending out a message saying "A supply ship is going to arrive at Liverpool on the 22nd", sending the ship to Cardiff instead, and then making sure the Nazis intercept a telegram saying "Liverpool's docks got damaged in a fire, go to Cardiff instead"

The best example of a "Nazi spy" was Juan Pujol García, a Spanish spy.

he independently decided to become a double-agent, so he pretended to be a pro-Nazi Spanish government agent, and convinced the Nazis to hire him as a spy.
They told him to go to the UK and recruit more local British agents to spy for the Germans

So instead he moved to Lisbon, and bought a tourist guide to Britain.
He reported having recruited Brits to help him spy, and send along reports of their discoveries, including blaming them for all any incorrect information that came through.

Meanwhile the Nazis are considering him one of their best agents, and paying him and all his imaginary recruits for all their great intelligence, none of which is true.

He'd applied to the allies to be a spy several times already, but they'd turned him down.

Meanwhile they are trying to figure out why the Nazis still think they have a network of spies in the UK: Because of Double-Cross they know they have captured all the Nazi spies in the country. So who the heck is this guy?

They figure out that it's just someone lying to the Nazis who isn't actually in the UK, and also realize how useful this is:
He'd just made the German Navy waste a ton of resources trying to find and sink an allied convoy... which didn't exit.

So they hire him, bring him to Britain (as well as his family), and start giving him resources to make this even more believable.

Things like telling him about actual operations, to let him leak it to the nazis slightly too late to be useful.

And having additional agents to write more communications back to the Nazis, making it more plausible that he had a whole network of nearly 30 agents

They even did things like cover for "mistakes" he'd made.
Like, when his "Liverpool agent" didn't tell the Germans about the big fleet movement leaving that port, he said that the agent had suddenly fallen ill, and a fake obituary was put in the newspapers

The German high command, of course, promised to pay a pension to the dead agent's widow.

After so many "just slightly too late" messages by airmail about allied activities, the Nazis decided he needed a radio.
So he "hired" a radio operator, and the Nazis sent over information on the encryption system he would use.

which of course was immediately handed over to the codebreakers at Bletchley Park.
This wasn't Enigma (it was a manual system), but was actually really helpful for further Enigma codebreaking

because he'd use this system to transmit messages to Madrid, then the agents there would decode them, then use Engima to re-transmit them to Berlin.
Which the allies could intercept

Which meant they had:
1. the encrypted Enigma transmission
2. the original plain-text version, because THEY WROTE IT

naturally this really helped with work on Enigma.

He was vital in the D-day deception, Operation Fortitude.
They specifically set it up to cause delays for accurate messages and to have inaccurate but-vaguely-close information.

The Nazis kept 2 armored divisions and 19 infantry divisions in Pas de Calais expecting that the "second invasion", the real one, the big one, was about to land. They kept them there until AUGUST. (D-day was June!)

Rommel is like "can I send those to Normandy, to fight the actual invasion?"
"no. Patton is about to send 75 divisions to invade Pas de Calais! Our best agent is certain of this."

A month after D-day they decorate him with an Iron Cross 2nd Class. This is one of the highest awards a non-German could get, and required personal authorization from Hitler.

And a few months later he gets an MBE from King George VI.
So he had both, making him one of the very few people to get decorated by both sides of WW2.

The war ends, and he dies, from malaria, contracted in Angola. How sad.

or not. He was a fucking spy. That was a cover story, the espionage version of witness protection. (There might still be Nazis around, after all, and some might figure out who he is)

In reality he retires to Venezuela, running a bookstore under a new name.

He actually died in 1988, at the age of 76.

During WW2, the Germans paid him a total of approximately 340,000$, to support him and his 27 ENTIRELY FICTICOUS agents (and their widows, of course)

It's not reported if the widows were fictitious as well, but I suspect so. Very few people marry imaginary nazi spies.
I don't think that was even legal in 1940s Britain.

Anyway there are a lot of pictures of him from his 1984 trip to the UK, to be honored by Prince Philip.

But the picture of him from 1931 when he was a conscript in the Spanish army definitely best fits his career, as someone who lied to the Nazis entirely on his own, without support from his government or any other (at first)

and why did he do that? why did he decide to risk his life to become a fake nazi spy, all on his own?

Anyway this whole thread was a tangent caused by an IRC conversation talking about the 8-bit-guy.

I need to go get some coffee and maybe turn down my ADHD from a 9 to maybe a 6 or 7.

So if you enjoyed this, feel free to send me a dollar or two on my ko-fi, to pay for the coffee!
https://t.co/fxSZjxyBm0

or do the patreon thing so you can send me some monthly dollars:
https://t.co/Sd9bKPHLf2

or if you want to read more twitter rant threads about random history things and computer and, like, star wars?
I've got a list of a bunch of 'em on my wiki:
https://t.co/zF7vci6gcy