Make Technology Great Again

slide 1

My name is Michał Woźniak, also known as rysiek,

slide 2

and I have 3 minutes to do a rant about how broken technology is. And broken it is!

One important note, I have about 50 slides for 3 mnutes, and I will be asking questions. I hope you've all had coffee!

slide 3

We all know and love Microsoft Office, one of the biggest security problems humanity has seen.

slide 4

How many of you use Microsoft Office daily?

slide 5

Who of you ever used Dynamic Data Exchange in MS Word? Or ActiveX? Or OLE?

slide 6

Well you'll be glad to know that this 30-year-old proprietary crap made you all vulnerabole to malware. You're welcome.

Anybody uses Microsoft Word on a Mac?

slide 7

Clearly that doesn't help that much.

slide 8

It's not like it's just about old tech, either. PowerShell is pretty new and is already being exploited.

Anybody ever connected a printer with their Windows system?..

slide 9

Any users of Microsoft Outlook perhaps?

slide 10

One might could think that antivirus software keeps us safe.

slide 11

One would be wrong.

So, Microsoft in decides to build their own antivirus that will solve all these problems.

slide 12

Anybody surprised by this? Of course not.

Any Apple users in the audience?

slide 13

This is a great one. You encrypt your harddrive using a strong password, and when you try logging in, lo and behold – in the password hint... the password.

slide 14

There's even an Apple Support article about this.

slide 15

There goes Apple security, right out the windows.

slide 16

These characters would crash any iPhone and iPad for a while.

slide 17

Or let's take Sony. Sony decided to distribute Windows malware to users machines so their CDs would not get copied.

Malware got distributed. But CDs got copied anyway, of course.

slide 18

Thankfully we're moving everything into the browser, and browsers are pretty secure – unless of course you're using Flash or Java.

Please do not use Flash nor Java.

slide 19

If you have a home router that you did not set up yourself, you are probably a part of a botnet. Congratulations.

slide 20

Or, if you have a "smart lightbulb", for that matter.

slide 21

If you have a WiFi-enabled entertainment center in your car, you might want to look into that.

slide 22

Because car manufacturers clearly did't.

slide 23

Oh, sniper rifles are Internet connected these days to. So are fish tank thermometers. So of course they get owned.

But off to the world wide web. Any of you host websites on Drupal? Joomla? Wordpress?

slide 24

But at least if we're using HTTPS the *connection* is secure, right?

slide 25

There are about 130 Certificate Authorities and any of these can issue certificates for any site. Many are government-controlled, in places like China or Russia.

Or, you know, have bad security.

slide 26

But even if certificates are not a problem, software that uses them is. Yay!

Having fun so far? Cool, let's talk about tech companies who manage your data!

slide 27

Like Equifax, who offer a service to protect your identity on-line.

It leaked your identity on-line.

slide 28

Then they tried to help you figure out if you were affected, but they did it so badly this new site got blocked.

As a suspected phishing site.

slide 29

And then at some point their main website started serving malware.

slide 30

Then there's Panera Bread, which got informed about a problem and failed to do anything for 8 months.

slide 31

But I guess that's par for the course since they hired a guy who used to work for Equifax.

slide 32

But telecoms! Telecoms know how to deal with security, right?

slide 33

Never do this by the way. Never keep clear-text passwords.

slide 34

slide 35

Or this. Never respond to a thread about your security by saying it's awesome.

Hey at least it's not 2008 anymore and we have some secure communication tools! Anybody here uses Telegram? Viber? WhatsApp?

slide 36

Well... Anyone here using Signal?

Cool carry on, Signal's actually secure.

slide 37

Yahoo on the other hand...

But perhaps we can find some hope in the tightly regulated industries? Banks?

slide 38

Air travel? Airports have to be pretty secure, right?

slide 39

Well, not unless they're using Windows 3.1 for a fog navigation system. Not 3.11, by the way – 3.1!

slide 40

Now, there is a lot of money in securing stuff. Computer Emergency Response Teams are the ones doing the most important work, but they're not getting bulk of the money.

Big money goes to NSAs and CIAs of this world...

slide 41

Which lose cabin pressure...

slide 42

...their tools get posted on the open Internet...

slide 43

...and we get the first US tax dollars-supported ransomware attacks. Your tax dollars at work!

slide 44

Here's a partial list of cyberattack groups supported by government and government-like entities. They specifically do *not* keep you safe!

slide 45

Oh, in case you thought we should turn our hopes towards the private sector. Hacking Team and Gamma International are in the business of making surveillance tools and malware.

slide 46

They always claim they do due dilligence and never sell to regimes. I direct your attention towards the "on-site assembly in Turkmenistan" line on their leaked invoice and call bullshit on their due dilligence claims.

slide 47

And finally, no, we cannot even trust our CPUs, the most basic components of our computing devices. There's a bug in every modern CPU manufactured during the last 20 years. It's unfixable...

slide 48

...and exploitable via a browser.

slide 49

sips from a flask

So here's the problem: best and brightest minds of our generation are hard at working getting people to click 1% more ads on Facebook or creating a new blockchain scam.

slide 50

And there is no engineering in software engineering.

We keep rebuilding everything from scratch, reinventing the wheel, all the time. C, C++, Java, Python, Ruby, JavaScript... redoing all libraries in the new language means we do not have time for security.

slide 51

We need to fix the development process, so that software starts being *made* in a secure way.

We need to dismantle the vendor lock-in so that people can switch software based on things like security, instead of being locked to shitty solutions of the Microfaceboopple of this world.

We need to educate people so that they don't fall into vendor's traps and *demand* security, interoperability, etc.

Above all we need to change incentives. Dramatically.

slide 52

The Free Softwrae community is already hard at work regarding the development process. I won't go into gritty details, but it's happening.

slide 53

For that to happen we need to make sure people can switch away, easily, from insecure solutions. Right now they really can't (or at least they feel they can't).

In order to achieve this we need open protocols and open standards. So that it doesn't matter what kind of software and operating system you're using to edit your document. So that security is no longer an afterthought.

slide 54

What we're dealing with is basically "insecurity as a business model".

Companies focus on (proprietary) features, because that's what they can put in bullet points, that's what draws in the users – and locks them to a platform.

Switching to other, perhaps more secure software becomes hard, since it does not support these features.

But also, these features are implemented badly, without security in mind. They become riddled with security problems.

Still, products get sold, and the cycle repeats itself.

slide 55

Think of Microsoft's OLE, ActiveX, DDE, etc.

Who's paying for Microsoft's lack of security? Users. You. Because it's hard for you to switch. Because of proprietary bullcrap.

slide 56

Think of Intel's "optimizations" that led to Meltdown and Spectre.

If performance drops 20-30% in datacenter uses, what will datacenters do? Buy more CPUs? From whom? From Intel!

slide 57

Think of Facebook. There is outrage now, as it has been in the past. What do people do? They set up Facebook groups to express their outrage. This is called Stockholm Syndrome. This is you vs. the tech industry today.

Why can't we standards that make it possible for users of Facebook, Twitter, and other social network operators to talk to each other just like users of one mobile operator can talk to anyone using any other operator?

We can. We actually have ActivityPub, we've had OStatus for a decade or so. But Facebook will not implement them, because their business model depends on keeping users locked in their walled garden.

Make no mistake! Facebook's, Micropsoft's, etc. actions are not "missteps", they are execution of their business model strategies. And implementing open standards is not happening because it's hard – Microsoft's own OOXML format is over 6000 pages, ODF is just a bit over 100! It's because it is not compatible with their business model.

Let me repeat: your security and ability to choose software providers is not compatible with these companies' business models.

slide 58

Remember Internet Explorer 6? That was a nightmare. Both security-wise, and usability wise. But we could not move users off of it because it butchered the open standards of the open web and so sites were built for it and didn't work in standards-compliant browsers.

Only when Mozilla Firefox started gaining traction, Microsoft started fixing their crap. It wasn't happening before not because it was hard – as Firefox proved – but because it was not compatible with business model of locking people up.

And now we have a pretty good set of browsers whose security is quite okay. Firefox, Chrome, even MS Edge. Only because Mozilla had the audacity to try to break the monopoly.

We need more Mozillas. And we need to support them.

slide 59

That's where education comes in. We need to teach people to use more than one operating system. When learning to drive, I was taught how to drive, not how to drive a Toyota or a Ford.

Why are we teaching kids how to use a particular office suite? A particular operating system? How does any of this make sense?

And we need to teach kids about information security and operational security in schools. Just like we teach tem to look around when crossing the street. Companies like Facebook made the generation gap into a business model. They are monetizing on the fact that we are not teaching kids how to be safe online.

All of this is called media education. It also includes figuring out what is true and what is not on the Internet. You want to fight Fake News, also known as Propaganda? Teach kids logic, teach kids how to check sources in schools. Teach media education.

Do we need some programming in schools? Sure, but just a bit. Just enough to show kids computers are not magical black boxes. They are tools. Tools we can and should control.

slide 60

We need to change the incentives. For the whole industry. We need to turn them upside down.

slide 61

That means regulating the tech industry. And I hate the sound of it too. But clearly Microfaceboopple is not going to fix itself, and the only entities that have enough power – hopefully still! – are governments. So we need to rely on them.

The way I think about it is that even with all problems with democracy we still get to vote every few years. We have no say, no vote in what Facebook does. And we feel we can't "vote with our feet" due to vendor lock-in.

If anyone wants to try, join me. I don't have a Facebook account, never had. I closed my Twitter account 5 years ago. But I have a very active Mastodon account – and that's a decentralized, standards-based social network.

We also need to fix the cybersecurity agencies and the surveillance industry, they are doing more harm than good. Move those billions of dollars from supporting hoarding of vulnerabilities and buying stuff from Hacking Team or Gamma International to CERTs and other orgs who will help vendors fix their software.

slide 62

So, how should we regulate?

Mandate or at least strongly support open standards and open protocols, so vendor lock-in becomes less of a thing.

Introduce warranty and liability for closed-source software and any software solutions that are paid for in any way.

Put "best before" date on hardware like routers, "smart" TVs, smartphones, etc. Make full updates and support mandatory until the best before date. After it mandate that code must be released as open source, or otherwise the vendor remains liable for it.

Put labels akin to "food safety labels" on software. "This shoftware sends data to third parties", "this software relies on Google infrastructure", etc. So that customers can really make informed choices. Standardize these labels so that customers don't have to wade through 200 pages of text.

slide 63

Deal with the cybersecurity agencies. Change focus from offence to defense. Force them to work with vendors, mandate they have to inform vendors about known vulnerabilities and help fix them.

Make them liable for any offensive tools we can attribute to them that leaks and is used in malware.

slide 64

Fix the surveillance industry.

Control their products like weapons sales and exports. Create explicit regulation on how these products can be deployed and what kind of due process needs to be followed, what reporting needs to be done. These are akin to wiretaps, and that's how they should be regulated.

Enforce all of this in an effective manner.

slide 65

And do not, under any circumstances, do any of these!

These will make everyone less secure. It will get journalists and their sources killed. It will give carte blanche for authoritarian regimes to censor and surveil their citizens, pointing towards the UK as a shining example.

Do not prosecute security researchers who coordinate disclosure with vendors in a responsible way. Security research is already hard enough without the threat of jail showing up at the end of it.

Do not cripple security research to protect dying business models. DRM does not work. Badly done DRM makes everyone vulnerable, as Sony DRM showed. Researchers need to be able to legally poke it and probe it's security.

slide 66

There is some hope. But there is not much of it.

EU sometimes has some good ideas. I hear there's a company opening their source code on this conference this Saturday.

Support such initiatives. Call your MEP. Now you know what I know; It's on you now. Nobody else will do it for you.

Be the solution you want to see in the IT world.