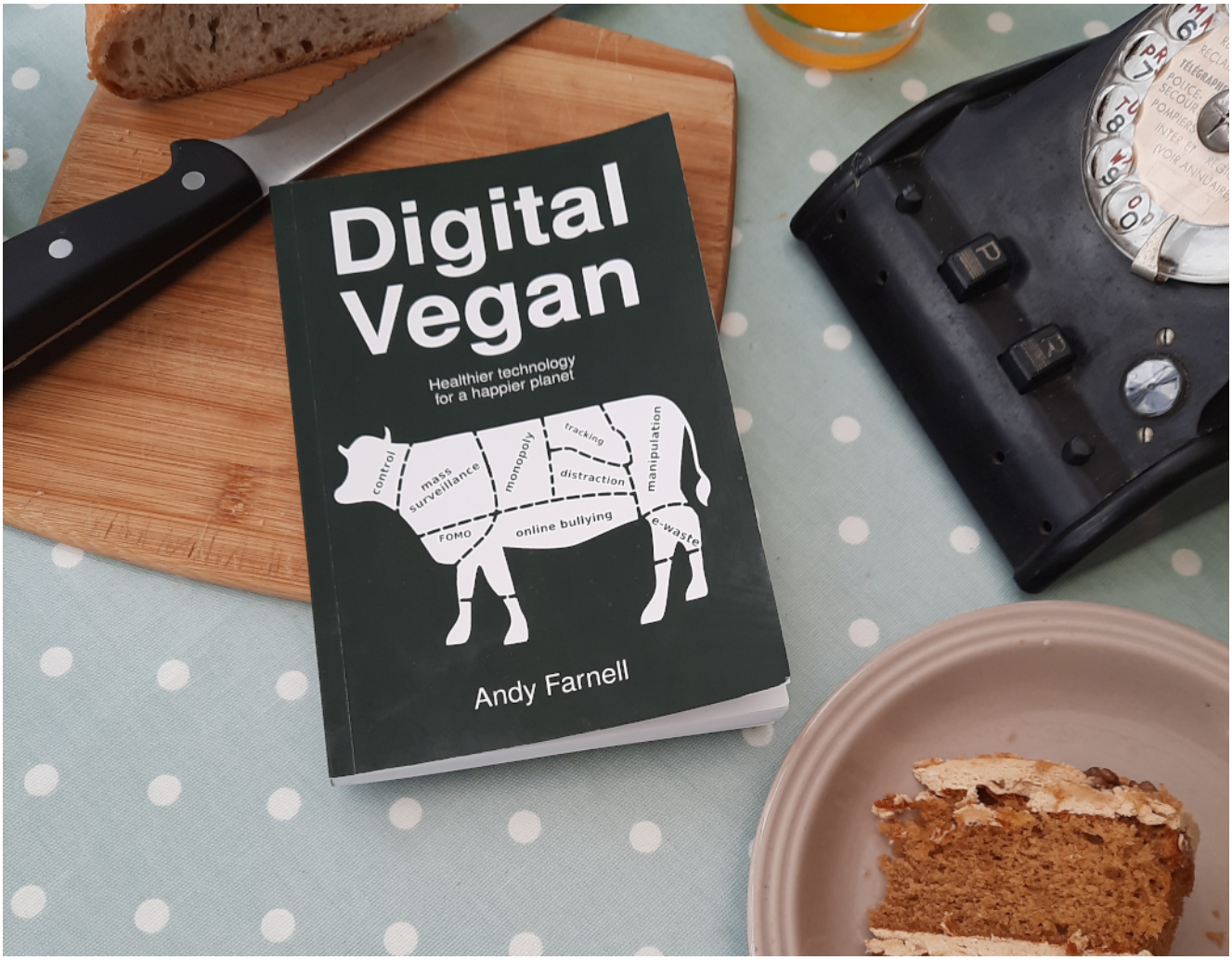
Why We Can't Teach Cybersecurity

By *Roy Schestowitz*
Created *29/11/2021 - 12:52am*
Submitted by Roy Schestowitz on Monday 29th of November 2021 12:52:22 AM Filed under Linux [1]

By Dr. Andy Farnell



I teach cybersecurity. It's something I really believe in, but it's hard work for all the wrong reasons. First day homework for students is watching *Brazil*, *No Country for Old Men*, *Chinatown*, *The Empire Strikes Back*, or any other film where evil triumphs and the bad guys win. This establishes the right mindset - like the medics at the Omaha beach landing in *Saving Private Ryan*. Not to be pessimistic, but cybersecurity is a lost cause, at least as things stand today. If

we define computer security to be the combination of confidentiality, integrity, and availability for data, and as resilience, reliability and safety for systems, then we are failing terribly on all points.

As a "proof" after a fashion, my students use a combination of Blotto analysis from military game theory, and Lubarsky's law ("there's always one more bug"). It is a dispiriting exercise to see how logic stacks up against the defenders, according to which "the terrorists always win". Fortunately, game theory frequently fails to explain a reality where we are not all psychopathically selfish Bayesian utility maximisers (unlike corporations which are programmed to be). Occasionally hope, compassion, gratitude, and neighbourly love win out.

Could things be worse than having mathematics against you? Actually yes. You could live in a duplicitous culture antithetical to security but favouring a profitable facsimile of it. Perhaps that's a means for obsolete power hierarchies to preserve themselves, or because we don't really understand what "security" is yet. Regardless, that's the culture we have, and it's a more serious problem than you might think, much more so than software complexity or the simple greed of criminals.

My optimism is that if we can face up to facts, we can start to change and progress. It is in the nature of teachers, doctors and drill instructors that we *must* believe people can change. So I'll try to explore here how this mess happened, how Linux, BSD and free open source software with transparent standards are a plausible even necessary way out of the present computer security crisis, and why the cybersecurity courses at most universities are not helping.

We have to keep faith that complexity, bad language design and reckless software engineering practices are surmountable by smart people. Maybe one day we'll build computers that are 99.9% secure. But that is unlikely to happen for reasons recently explained by Edward Snowden, who describes an *Insecurity Industry*. Indeed, I was a little disappointed by Snowden's essay which does not go nearly far enough in my opinion.

For me, the *Insecurity Industry* is not located in a few commercial black-hat operations like Israel's NSO Group, but within the attitudes and practices running through every vein of mainstream computing. As with its leaders, a society gets the technology it deserves. As we revel in cheap imported goods, surveillance capitalism, greed, convenience, manipulation, and disempowerment of users, we reap the security we deserve.

Blaming the cyber-arms trade, the NSO or NSA for answering the demands of cops and criminals alike, is distracting. Without doubt what they are doing is wrong and harmful to everyone, but we can't have secure computing while those who want it are an educated minority. That situation will not change so long as powerful and fundamentally untrustworthy corporations with business models founded on ignorance dominate our digital lives.

Projects of digital literacy started in the nineteen eighties. They kick-started Western tech economies, but faltered in the mid nineties. Programming and "computer studies" which attempted to *explain* technological tools were replaced by training in Microsoft Word and Excel spreadsheets. Innovation tailed-off. A generation taught to be dependent on tech, not masters of it, are fit only for what David Graeber described as *Bullshit Jobs* Graeber18.

Into this vacuum rushed "Silicon Valley values" of rent seeking, piggybacking upon established standards and protocols. With a bit of spit, polish, and aggressive marketing, old lamps could be foisted upon consumers. Twenty years later we have a culture of depressed, addicted, but disenfranchised technology users Lanier11.

We have moved from "It's more fun to compute" to "If you've nothing to fear you've nothing to hide". In other words, we've transformed digital technology from a personally empowering choice into systems of near-mandatory social command and control (see Neil Postman's *Technopoly* postman93). What advantage would any group have in securing their own chains and the weapons ranged against them? A sentiment only half-disguised in young people today is utter ambivalence toward tech.

As states move to reclaim control from social media platforms, public debate has been framed around whether Facebook and suchlike are threats to democracy and ought to be regulated. But this is merely a fragment of a larger problem and of a discussion that has never been properly widened to examine the general dangers of information

technology in all its manifest forms, in the hands of governments, businesses, rogue groups and individuals alike.

For me, an elephant in the room is the colossal distance between what we teach and what we practice. Twice convicted monopolists Microsoft set back computing by decades, and in particular their impact on security has been devastating. Yet their substandard wares are still pushed into schools, hospitals and safety-critical transport roles. Even as embarrassing new holes in their products are exposed daily, lobbying and aggressive misinformation from Microsoft and other Big-Tech companies, all of which suffer from appalling privacy and security faults, continues unabated.

Big-tech corporations are insinuating themselves into our public education and health systems without any proper discussion around their place. It is left to well educated individuals to opt-out, reject their systems, and insist on secure, interoperable choices. Advisories like the European Interoperability Framework (EIF is part of Communication COM134 of the European Commission March 2017) recognise that tech is set to become a socially divisive equality issue. The technical poverty of the future will not separate into "haves and have-nots", but "will and the will-nots", those who will trade their privacy and freedom for access and those who eschew convenience for digital dignity.

As the word "infrastructure" (really vertical superstructure) has slyly replaced ICT (a horizontal service) battles have raged between tech monopolies and champions of open standards for control of government, education and health. The idea of public code (see the commentary [2] of David A Wheeler and Richard Stallman) as the foundation of an interoperable technological society, has been vigorously attacked by tech giants. Germany fought Microsoft tooth and nail to replace Windows systems with 20,000 Linux PCs in 2015, only to have Microsoft lobby their way back in, replacing 30,000 desktops with Windows 10 in 2017. Now the Germans seem poised to switch again, this time taking back all public services by mandating support for LibreOffice.

In the UK, several institutions at which I teach are 'Microsoft customers'. I pause to use the term "Microsoft Universities", but they may as well be. Entirely in the pocket of a single corporation, all email, storage networks, and "Teams" communication are supplied by the giant. Due to de-skilling of the sector, the ICT staff, while nice enough people, lack advanced IT skills. They can use off-the-shelf corporate tools, but anything outside lockstep conformity allowed by check-box webmin interfaces is both terrifying and "not supported". I met a secondary school headmaster who seemed proud to tell me that they were not in the pockets of Microsoft, because they had "become a Google Academy". I responded that "as a Linux child", my daughter woudn't be using any of that rubbish either.

Here's a problem; I don't use Microsoft or Google products. At one level it's an ethical decision, not to enrich aggressive bullies who won't pay proper taxes in my country. It's also a well informed technical position based on my knowledge of computer security. For me to teach Microsoft to cybersecurity students would bring professional disgrace. I won't be the first or last person to lose work for putting professional integrity first. They say "Nobody ever got fired for choosing Microsoft". At some institutions that is not merely advice, it's a threat. Security in the shadow of Big-Tech now means job-security, as in the iron rice bowl from which the compliant may feed, but educated independent thinkers must abstain.

A more serious problem is not just that companies like Google and Microsoft are an expensive, controlling foreign corporations supplying buggy software, or that university administrators have given away control of our networks and systems, it's that commercial products are increasingly incompatible with teaching and research. They inject inbuilt censorship and ideological micromanagement into academies and schools.

Another is that "choice" is something of an illusion. Whatever the appearance of competition between, say, Apple and Facebook, Big-Tech companies collude to maintain interlocking systems of controls that enforce each others shared values including sabotage of interoperability, security and inviting regulation upon themselves to better keep down smaller competitors. Big-Tech comes with its own value system that it imposes on our culture. It restricts the learning opportunities of our kids, limits workplace innovation and diversity, and intrudes into our private activities of commerce and health.

In such a hostile environment for teaching cybersecurity (which is to teach empowering knowledge, and why we call it

"Ethical Hacking" 1) one may employ two possible methods. First, we can buy in teaching packages reliant entirely on off-site resources. These are the "official" versions of what computer security *is*. Two commonly available versions come from Cisco and the EC Council. Though slickly presented these resources suffer the same problems as textbooks in fast-changing disciplines. They very quickly go out of date. They only cover elementary material of the "Cyber Essentials" flavour, which ultimately is more about assurance than reality. And they are partial, perhaps even parochial versions of the subject arrived at by committee.

Online courses also suffer link-rot and patchy VM service that breaks lessons. Unlike in-house setups, professors or students cannot debug or change the system, itself an important opportunity for learning. Besides, the track record of Cisco with respect to backdoors no longer inspires much confidence [3].

The other method is to create "suitcase data-centres". A box of Raspberry Pi single board computers saves the day! The Raspberry Pi Foundation [4], perhaps modelled after the early digital literacy drives of Acorn/BBC has done more for British education than any dozen edu-tech companies by promoting (as much as it can) openness of hardware and GNU/Linux/Unix software.

Junk laptops running Debian (Parrot Linux) and SBCs make a great teaching setup because a tangle of real network cables, wifi antennas and flashing lights helps visualise real hacking scenarios. Professors often have to supply this equipment using our own money. I rescued a pile of 1.2GHz Intel Atom netbooks from the garbage. Because we are not allowed to connect to university networks, 3/4G hotspots are necessary, again using bandwidth paid for out of my own pocket in order to run classes. Teaching cybersecurity feels like a "forbidden" activity that we sneakily have to do despite, not because of, university support.

Teaching cybersecurity reflects a cultural battle going on right inside our classrooms. It is a battle between two version of a technological society, two different futures. One an empowering vision of technology, the other a dystopian trap of managed dependency. Dan Geer, speaking in 2014 [5] described cybersecurity as a manifestation of Realpolitik. Nowhere does the issue come so clearly to a head as in the schism between camps of Snowden or Assange supporters and the US State, each of which can legitimately claim the other a "traitor" to some ideal of "security".

At the everyday level there is a tension between what we might call real versus fake security [6]. The latter is a festival of form over function, a circus of phones, apps and gizmos where appearance triumphs over reality. It's a racket of productised solutionism, assurance, certification and compliance that's fast supplanting *actual* security efforts. By contrast, the former is a quiet anathema to "security industry" razzle. It urges thoughtful, modest simplicity, slow and cautious change. It's about what you don't do.

So, in our second lesson we analyse the word "security" itself. Security is both a reality and a feeling [7]. There are perhaps masculine and feminine flavours of security, one following a military metaphor of perimeters, penetration and targets, the other, as Eve Ensler Ensler06 and Brene Brown Brown12 allude, an inner security that includes the right to be insecure and be free from patrician security impositions "for your own good". Finally, there is the uncomfortable truth that security is often a zero-sum affair - your security means my insecurity. While "good" security is a tide that raises all ships, some people misuse security as a euphemism for wielding power.

None of these social and psychological realities fit well into the lacklustre, two dimensional models of textbook computer security. Fortunately a mature discipline of Security Engineering which does not dodge social and political factors has emerged in the UK. Ross Anderson Anderson08 is part of a team leading such work at the Cambridge Cybercrime Centre [8]. One take-away from lesson two is that the word "security" may not be used as a bare, abstract noun. One must ask; security for who? Security from who or what? Security to what end?

Once we begin to examine the deeper issues around device ownership, implied (but infirm) trust models, forced updates, security theatre, and conflicting cyber-laws, we see that in every important respect tech is anarchy. It's a *de facto* "might is right" free-for-all where much of what passes for "security" for our smartphones, online banking and personal information is "ignorant bullshit" (in the strict academic sense of bullshit according to Harry Frankfurt; that

vendors and politicians *don't know that they do not know what they are talking about* - and care even less Frankfurt05).

Consequently, much of what we teach; the canonical script of "recon, fingerprinting, vulnerability analysis, vector and payload, clean-up, pivoting, escalation, keeping root?", and the corresponding canon of blue team defence (backup, intrusion detection, defence in depth, etc?) - has no context or connection to a bigger picture. It is ephemeral pop that will evaporate as technology changes leaving students with no deeper understanding of what we are trying to do by testing, protecting and repairing systems and data, or why that even matters.

We create more guards for the castles of tech-feudalism - obedient, unthinking security guards employed to carry out the whims of the management class. Leveraged by the unspoken carrot of preferential technical privilege and enforced by the stick of threatened removal of their "security status", they become administrators of new forms of political force. Challenges to grey-area behaviours beyond the legal remit of managers, are proclaimed "security breaches" unless pursued through intractable administrative routes or through appeals that can be deflected with allusions to "policy" or the abstract "security" of unseen authorities. Some of our smartest people are ultimately paid well to shut up and never to think for themselves.

There is a very serious concern that our "Ethical Hacking" courses (which contain no study of ethics whatsoever) are just creating fresh cyber-criminals. Despite the narrative that "we are desperately short of cybersecurity graduates and there are great jobs for everyone", the reality is that students graduate into an extremely competitive environment where recruitment is often hostile and arbitrary. It doesn't take them long to figure that their newfound skills are valuable elsewhere.

Years ago, it became clear to me that we must switch to a model of "Civic Cyber Security". I became interested in the work of Bruce Schneier not as a cryptographer but as an advocate of Technology In The Public Interest. National security is nothing more than the sum-total of individual earned and learned security. That means teaching children as young as five foundational attitudes that would horrify industry.

There is no room to lie back and hope Apple or Google can protect us. Organisations like the UK's National Cyber Security Centre, or US National Security Agency, which have conflicted remits, might wish to be seen as benevolent guardians. Their output has been likened by comedian Stuart Lee to "Mr Fox's guide to hen-house security". Cybersecurity can never be magically granted by those who have a deep and lasting interest in withholding it.

The business of "personal computing" has become ugly. Cybersecurity, in as much as it exists, is a conflicted and unreliable story we tell ourselves about power and tribal allegiances. We can't put on a "good guys" hat and beat "cyber-criminals" so long as we are competing with them for the same thing, exploitable clueless users.

The only questions are whether they are to be sucked dry by ransomware, "legitimate" advertising, or manipulated for political ends. If we are to engage in sincere, truthful education, then we have to call-out Big-Tech for what it is; more a part of the problem than a solution. Those of us who want to explore and teach must still circumvent, improvise and overcome within institutions that pay only lip service to authentic cybersecurity because they are captured by giant corporations

Bibliography

Bibliography

- [Graeber18] David Graeber, Bullshit Jobs: A Theory, Simon and Schuster (2018).
- [Lanier11] Jaron Lanier, You Are Not a Gadget, Vintage (2011).
- [postman93] Neil Postman, Technopoly: The Surrender of Culture to Technology, Vintage Books. N.Y.

(1993).
- [Ensler06] Ensler, Insecure at last, Villard (2006).
- [Brown12] Brené Brown, The Power of Vulnerability: Teachings on Authenticity, Connection and Courage, Sounds True (2012).
- [Anderson08] Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley (2008).
- [Frankfurt05] Harry Frankfurt, On Bullshit, Princeton University Press (2005).

Footnotes:

1 A term made up to attract young students to cybersecurity while assuring parents and politicians.

About the author

Dr. Andy Farnell is a computer scientist, author and visiting professor in signals, systems and cybersecurity at a range of European universities.

His recent book "Digital Vegan" [9] uses a dietary metaphor to examine technology dependency and over-consumption.

Linux

Links:
[1] http://www.tuxmachines.org/taxonomy/term/123
[2] https://publiccode.eu/
[3] https://www.schneier.com/blog/archives/2018/08/backdoors_in_ci.html
[4] https://www.raspberrypi.org/about/
[5] http://geer.tinho.net/geer.blackhat.6viii14.txt
[6] http://techrights.org/2021/10/12/citation-fake-security/
[7] https://www.schneier.com/blog/archives/2008/04/the_feeling_and_1.html
[8] https://www.cambridgecybercrime.uk/
[9] https://digitalvegan.net