Beef Jerky, Hoverboards and Hackers

By Misch Pautsch

Published on 15 Oct. 2021

Switch to German for original article

How do you reach a group of hackers? By mail, apparently. They respond - unsurprisingly - quickly. Or by visiting the officially reported headquarters of their asbl in Luxembourg City: The "Chaosstuff". This all doesn't sound as suspicious as the word "hacker" might suggest. A conversation with hobbyists.

The name Chaos Computer Club is mostly mentioned in the media when something goes wrong. In Luxembourg, this was recently the case when the data leak on the new website for online petitions was discussed. But also the Chamber leak affair in 2018 and in Germany the leak on the CDU's election campaign app in May 2021, both of which ended in – now withdrawn – legal action drew the attention of the CCC. In both cases, the Luxembourg and German Chaos Computer Clubs have each strongly criticized the legal action taken against the whistleblowers and have argued that those responsible for the sites should also take their responsibilities, rather than shooting the messengers.

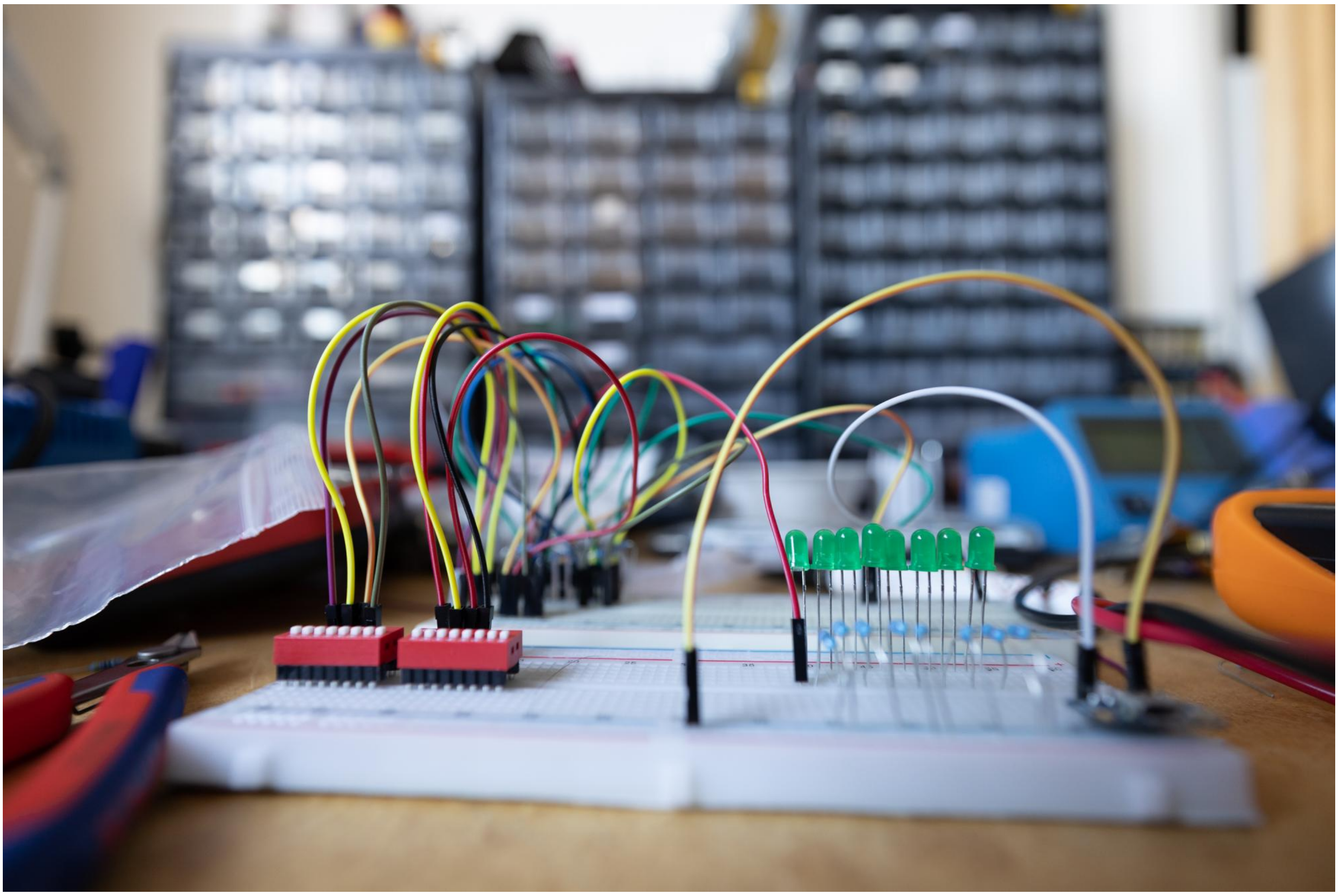
"These moments are probably the ones most people know us for", confirms Dennis Fink of Computer Club Luxembourg (C3L): "And it's certainly a big part of our work, possibly the most important, to educate people about technology, digitization, copyright, and privacy." However, when a group's name almost always comes up only in the context of negative news, that bitter taste sometimes risks rubbing off on those involved. It doesn't help that the term "hacker" is culturally loaded: There's something mischievous to thoroughly criminal attached to it, depending on the context."

Dennis Fink

"Whenever people talk about a hacker attack in the press", Fink laments, "they're talking about what we call 'crackers'. That is, individuals or groups who derive personal benefit from often criminal attacks. 'Blackhats', as many call them." This is a reference to classic Western movies, in which the villains usually wore black cowboy hats and the heroes wore white ones. "Now we're not quite 'whitehats' – those IT professionals who work for security companies or the state, for example – but, rather, "greyhats", so we have a critical attitude toward the state, while standing up for people's rights."

Repurposed

Public relations is certainly the most prominent part of the association, but it's just one of many, less headline-grabbing ones. The members of C3L are "hackers" in the classic sense: they are tinkerers. The first self-proclaimed hackers were the students in the "Tech Model Railroad Club" at MIT (Massachusetts Institute of Technology). The name is not a clever cover story for shady actions in a club room. No, the group was a collection of miniature railroad enthusiasts who gradually expanded their hobby with "hacks", technical solutions to difficulties they encountered while tinkering.



The C3L, like all Chaos Computer Clubs, continues this tradition. If you use technology for something it's not initially meant for, you're hacking. "In that sense, we're definitely hackers. The best example is a dehumidifier in our studio that is meant for making beef jerky. We use it to keep dry the material we need for the 3D printer. It reacted to high humidity, so we needed a solution. A hack."

Just as in the Tech Model Railroad Club, which has gradually moved more toward IT to further automate its own models, in C3L anyone can talk about their interests. "That goes from best practices for growing chilies – that was a bigger project – to a rolling board that we converted with the parts of a hoverboard so we can control it remotely, to the nerdiest discussions about parameters in encryption algorithms", Fink explains. For many, however, the issue of IT security and privacy remains at the core of C3L.

"Above it all, along with hacker ethics, is one 'rule': be excellent to each other. Our common goal is to help society, advocate for freedom of information and protect private data." According to Fink, a pivotal moment for the collaboration with public stakeholders was two video conferences with political parties, where the group was able to share their opinion on the proposed copyright reform. "Several MPs had already asked parliamentary questions in response to our press letters before, but of course we hope that this development will continue in the direction of dialogue. On copyright reform, for example, as far as I know, at the moment it looks like our feedback has not led to any change. Not a lot of brainpower has gone into many of the sections, in my view."

"You wouldn't give a stranger your credit card."

Dennis Fink, C3L

Another development that C3L is watching with a critical eye is the rapid development of biometric data collection and recognition. At the EU level, a ban on technologies that could identify people by their gait, posture, typing behavior or facial recognition, among other things, has been discussed for some time. However, a final decision on further action has not yet been made. "We see a tendency that such systems can and will also be built into surveillance cameras. Movement profiles will be able to be recognized even better and in two or three years it will probably be possible to capture emotions. At the same time, we see that cameras are being plastered everywhere..."

Online

Fink does not accept the eternal argument that those who do nothing wrong have nothing to fear. The advocates of data protection have heard the same old story too often, not to have an answer at the ready: "You also close the toilet when you go to the bathroom at home. That's a bit crass, of course, so in other words: You wouldn't give a stranger your credit card, either." Having data about people lends power; it's not for nothing that the market for consumer behavior has become one of the most important areas of commerce at the latest since social media penetrated every stage of life: It's the business of Facebook and Google, the titans of the digital revolution. And increasingly a tool of social control.

"Why should a state be allowed to do what others are not?" asks Fink. "A lot of people don't realize what privacy brings to us and to all of humanity every day. It allows us to flourish, to be who we are. Take depression, for example. Not everyone needs to know when someone has a mental health condition. Neither the government nor the health insurance company." That costs for insurance, for example, go up "because everyone knows everything about you, we think, doesn't have to be."

Even those who blindly trust big data collectors, be they governmental or private, would do well to hope their information doesn't fall into the wrong hands. Like, for example, during a series of ransomware attacks on hospitals in the United States. Crackers blocked their computer systems, sometimes for days, which not only delayed the treatment of many patients, but also, according to spokespersons for the affected hospitals, significantly increased the mortality rate during that time.

Investigators suspect Russian gangs with state support behind the attack, which was not to remain the only one: Similar attacks crippled a Colonial pipeline on May 7, 2021, and then, a little later on June 1, JBS, the largest meat products processor in the U.S.

One click?

"Do you know that every electricity meter in Luxembourg and most in Europe are connected to the Internet? 'Smartmeters'." Fink raises his eyebrows. "They're super cool, of course. You can read how much you use and when, they can be integrated into smart grids that make the electricity network more stable. Except, unfortunately, they have a catch. The operator can just turn off", he snaps his fingers, "like this. At a distance. They normally do not do that, of course. But since they're connected to the Internet, the Internet is connected to them. It only takes one person to find a security hole to cut off power to all of Luxembourg if they feel like it", the C3L posits.

"Why can't these networks be hooked up to another network? The same is true for hospitals. Why do these computers all have to be connected to the Internet? With some infrastructure, of course it's necessary, but all of it all the time? Why not create an intranet? Or, as we sometimes jokingly say here, a 'Luxembourg-net'? Of course, it would be more expensive, but better that than live with the fear that one person can sabotage the power grid across Europe."

The concept of data sparsity is central to IT security and, Fink believes, should be demanded more as well. One of the central questions in the Chamber leaks was why the sensitive data was on a publicly accessible server in the first place, Fink says: "On a server that is connected to the Internet, only the data that is necessary should be there." Once something is on the Internet, it's not forgotten. "That's why we look at each of these situations like a little battle, where we try to counteract decisions that we see as problematic. Some battles we win, some battles we lose."

As long as there are vested interests trying to restrict privacy, keep backdoors open, and force potentially dangerous technologies on Internet users, the hackers will keep an eye on developments. And in between, they'll talk about how best to water chilies.