FEBRUARY-APRIL 2018

CW Benelux

The quarterly magazine from Computer Weekly, focusing on business IT in Belgium, the Netherlands and Luxembourg

M-A-U/GETTY

Happy hacker

Dutch IT expert on a mission to expose vulnerabilities

CWBenelux

Computer Weekly,
25 Christopher Street,
London EC2A 2BS

General enquiries 020 7186 1400

EDITORIAL

Editor: Karl Flinders
020 7186 1423 | kflinders@techtarget.com

Editor in chief: Bryan Glick
020 7186 1424 | bglick@techtarget.com

PRODUCTION

Production editor: Claire Cormack
020 7186 1461 | ccormack@techtarget.com

Senior sub-editor: Bob Wells
020 7186 1462 | rwells@techtarget.com

Sub-editor: Jaime Lee Daniels
020 7186 1417 | jdaniels@techtarget.com

Sub-editor: Ryan Priest
020 7186 1420 | rpriest@techtarget.com

SALES

Sales director: Jat Hayer
07557 433681 | jhayer@techtarget.com

Published by TechTarget

275 Grove Street, Newton, MA 02466

www.techtarget.com

About TechTarget

TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.

TechTarget

Security fears call for digital vigilance

The word "hacker" carries with it negative connotations, but it needn't be that way. In fact, hackers could be the good guys who protect the world from the bad guys as it digitises.

This is nothing new. Ethical hackers have been plying their trade for years, attacking systems to find weak spots and informing target organisations when they do. This is vital because there are people out there doing the same but without good intentions.

In this issue, read about how and why one public sector IT professional in the Netherlands, Victor Gevers, took a whole year out to hack ethically and, in the process, unearthed almost 1,000 vulnerabilities.

Although his hacking sabbatical ended over a year ago, Gevers' mission is not over. He is a sought-after public speaker who shares critical insights about IT security.

But ethical hackers are not alone in revealing security flaws. In this issue, also read how journalists have brought security weaknesses in the Netherlands government to public attention. Reporters demonstrated how the email addresses of Dutch politicians are easy to spoof. A heated debate across the country followed about the responsibilities of reporters in revealing security flaws, and the implementation of common security practices on email servers.

Reporters demonstrated how the email addresses of Dutch politicians are easy to spoof

The furore began when Dutch investigative journalists from a website that specialises in financial news stories posted an article about the possibility of spoofing emails sent in the name of Dutch MPs. Reporters found it was possible to send emails that appeared to come from the domain used by the Netherlands parliament.

In the wider continent, policymakers in Brussels have approved a new electronic system to store biometric information on all non-EU citizens travelling in and out of the bloc. The entry/exit system (EES), as it is known, is part of the EU's so-called Smart Borders package, and will consist of a central database storing the name, travel documents, fingerprints, facial image, date and place of entry, exit and entry refusal of every third-country national. ■

Karl Flinders, editor

Dutch IT expert takes a hacking sabbatical

Ethical hacker Victor Gevers discovered nearly 1,000 vulnerabilities after taking a year off from his job in the Netherlands government to set up a hacking group. Jasper Bakker reports

What kind of person takes a sabbatical to do more work instead of less? Who chooses not just more work, but possibly thankless work and an uphill battle? A man with a mission – that's who.

Dutch ethical hacker Victor Gevers took full-time leave from his IT job in 2016 and used the time to hunt for vulnerabilities – anywhere, any time, anyhow. His mission was not just to hack around, but to find vulnerabilities, report them responsibly and then, hopefully, get them fixed by the vulnerable parties involved.

So, not a hacker in the cyber criminal sense, and not a hacker in the sense of shaking digital trees to see what falls out. No, this hacker is a concerned digital citizen. Gevers – better known by his online handle 0xDUDE – wants to make the internet, and therefore the modern world, a safer place. Seriously.

Gevers' endeavour echoes a similar effort by a Netherlands IT news website six years ago. *Webwereld*, a Dutch-only publication of IT content publisher IDG, declared October 2011 to be "Lektober", which translates as "Leaktober". Dutch security expert Brenno de Winter was the public face of a month-long daily publication of information leaks obtained via IT vulnerabilities.

A concerned digital citizen: Victor Gevers

GDI FOUNDATION

Previously, De Winter had become known for exposing fundamental flaws in the Netherlands' chip card for public transport. The security of the so-called OV-chipkaart was initially faulty, despite denials by card issuer Trans Link Systems. This led to a loss of public trust in the chip card, parliamentary questions, and eventually measures to improve the security of the payment card. All this was achieved after much controversy, interwoven with successful (and easy) hacks, and threats of lawsuits.

THE OVERALL GOAL WAS TO MAKE PEOPLE, COMPANIES, ORGANISATIONS AND GOVERNMENT BODIES AWARE OF VULNERABILITIES

October 2011 saw the start of an intensive campaign in which volunteer hackers reported vulnerabilities. They did so through an intermediary, who gave Webwereld the technical details. Then the editorial staff at the Dutch IT news website would inform the data-leaking organisations and urge them to fix the vulnerabilities, so that the cases could be publicised after they had been fixed.

The overall goal was to make people, companies, organisations and government bodies aware of vulnerabilities – both their own and those of others. Since that campaign, some progress has been made. The reporting of vulnerabilities via an intermediary – and employing journalists to inform vulnerable organisations – was necessary because the Netherlands lacked procedures for responsible disclosure. Nowadays, it has official guidelines for, and practical experience with, responsible reporting of vulnerabilities.

But this does not mean that the world, or the Netherlands, has achieved secure IT. The base level of security might have improved, but dependence on IT has grown significantly since then. Opportunities to gain by abuse and misuse of IT have also grown – so have the risks.

Senior security specialist Gevers is keenly aware of this. Besides being an innovation manager in the Netherlands government, he is also an ethical hacker who had reported 4,000 vulnerabilities in 16 years. But then he decided that ethical hacking needed more time and attention – at least a year of full-time attention, in fact.

GDI Foundation created

So, with colleague Vincent Toms, Gevers created the non-profit GDI Foundation to actively work towards a safer internet for everyone, everywhere. "To protect you, me and our kids. And prevent any misuse of information," states the organisation's FAQ. And in contrast to many well-meaning initiatives, lobby organisations and IT efforts, the GDI Foundation set out to do some actual hacking.

Well, not actually performing digital break-ins and stealing data, because that would be illegal. Its mission was to scan for "hackability", map out vulnerabilities and advise affected organisations on how to fix them.

The foundation relies on contributions from donations, sponsorships and participating members. This enabled Gevers to take

a year off work to focus solely on finding and reporting vulnerabilities, and 1 January 2016 marked the start of Project 366 – named after the number of days in leap year 2016.

Somewhat similar to 2011's Leaktober, this year-long security campaign targeted low-hanging fruit, as cyber criminals do. These vulnerabilities are easy to reach and yield relatively big rewards for malicious hackers – simple security problems that can cause a lot of trouble and damage.

Broad range of targets

The range of targets for Gevers' hack sabbatical was broad, ranging from FTP servers, NAS devices and MongoDB databases with unintentional wide open access, to vulnerable computers connected to critical infrastructure, as well as data-leaking consumer electronics.

In the first month alone, Gevers found and reported no fewer than 170 vulnerabilities, and the total for the year-long hack sabbatical was 960. In among all this hard work, Gevers received the Digital Impact Award from Dutch IT trade organisation Nederland ICT and the ECP (Platform for the Information Society).

His year-long hack effort concluded on 31 December 2016. But, just as with 2011's Leaktober, the world has not yet been secured. Certainly, the hard work of Gevers and Toms has made many systems more secure, but there is still much insecurity.

Fortunately, Gevers has not ended his mission. He has not only become a sought-after public speaker who shares his insights on IT security, but the ethical hacker and the GDI Foundation continue their work and have uncovered many more vulnerabilities, such as open access to MongoDB databases. They point to the example of a so-called NoSQL database that has been ransacked and ransomed in multiple waves of attack, hitting tens of thousands of installations.

Another example of the need for continuing vigilance over vulnerabilities was the discovery and reporting of open Jenkins servers. That open source automation software serves continuous delivery and DevOps, but can be wrongly configured and then hacked. Gevers found open Jenkins installations at Dutch hospitals last summer, with real medical data seemingly accessible.

In the first month alone, Gevers found 170 vulnerabilities, and the total for the year-long hack sabbatical was 960

Just two days later, Gevers discovered wide-open Telnet access to gain administrator rights on almost 3,000 Chinese bitcoin-mining machines. And in September, an international outreach was undertaken to inform internet service providers in dozens of countries that the Arris broadband devices they had supplied to their customers were vulnerable.

The list goes on and on, and the work to secure the internet goes on and on. Gevers' year-long hack sabbatical was impressive in its own right – but it was really just the start. ■

› Here are some pointers on how you can build your ethical hacker career

Belgian telco Proximus chooses Cloudify to support NFV roll-out programme

Belgium's largest telecoms operator will deploy a cloud-native orchestration platform to facilitate its adoption of network functions virtualisation services in the business, writes Alex Scroxton

Proximus, Belgium's largest telecommunications operator, will lean on orchestration specialist Cloudify to support its adoption of network functions virtualisation (NFV) as part of a multi-supplier team implementing its next-generation virtualised cloud network.

Using its cloud-native orchestration platform, Cloudify will help Proximus with NFV management and orchestration, and the on-boarding and deployment of virtual network functions (VNFs).

Proximus is using NFV to transform its legacy hardware-based network into a virtualised, cloud-native, software-driven domain that should be easier and cheaper to run.

React more quickly

In common with many other telcos that are dipping their toes into the world of NFV, Proximus's ultimate objective is to react more quickly to new trends, deploy new services and scale them, and improve its network security posture. "NFV adoption is a key component of our strategy for digital transformation, and Cloudify is helping us transform from traditional to virtualised networks that are simpler to operate, cost less to maintain and enable us to deliver better customer experiences," said Alex Thomas, programme manager for Cumulus and LPWAN (low-power wide-area network) at Proximus.

The project kicked off in earnest in 2016, and is currently working through the design, VNF onboarding and user acceptance testing phase ahead of delivering virtualised production services to Proximus customers this year.

Tosca standard

Cloudify will add its open source cloud management and network orchestration software, which features a number of NFV-specific plugins and blueprints to model VNFs and service function chaining based on the telco-friendly Tosca standard.

Cloudify claims to have the only open source NFV management and orchestration service that leverages Tosca's native, multi-VIM interoperability capabilities, and also boasts built-in

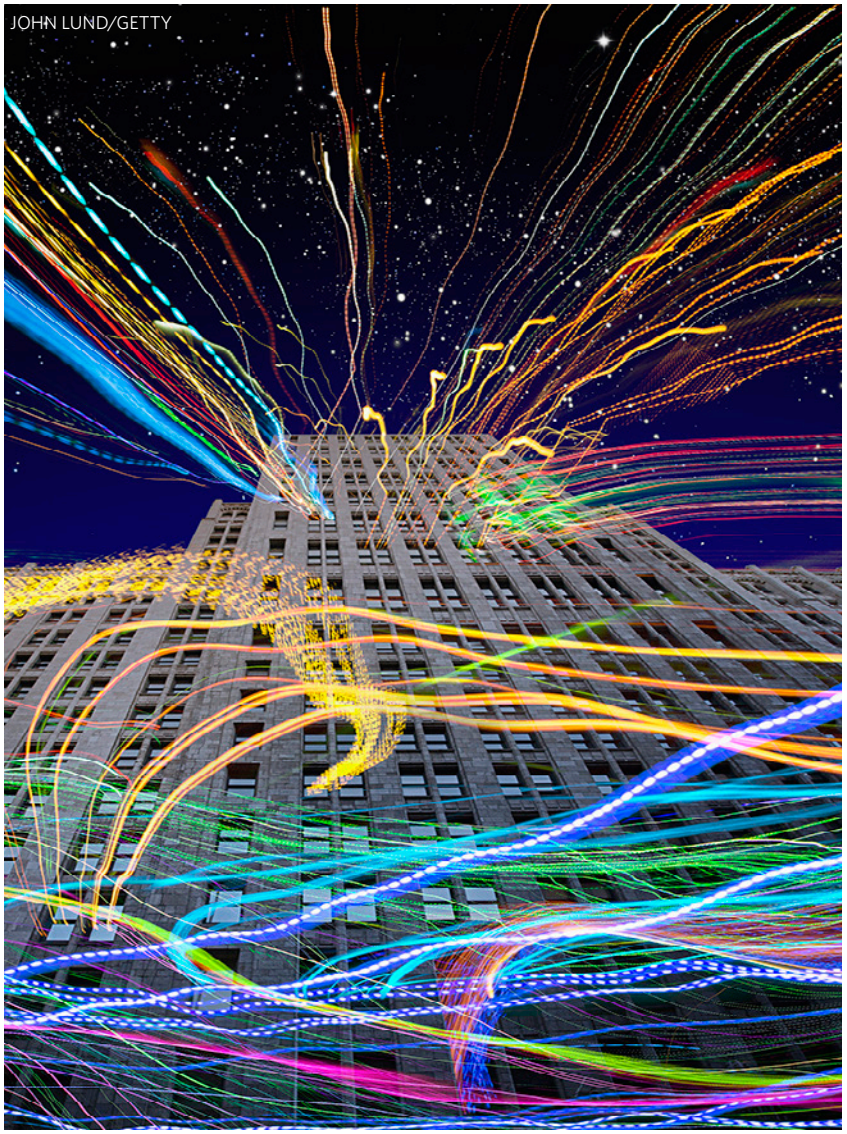
support and blueprints for OpenStack, and the entire VMware stack. "Cloudify's approach supports both physical network functions and VNFs, in software," said 451 Research research vice-president William Fellows. "This enables operators to optimise existing technologies while migrating toward the benefits of automation and DevOps best practices, without having to discard existing technology investments."

> **"We are lowering the adoption barriers for NFV by leveraging open source software that accelerates VNF onboarding while reducing technology risk"**
>
> Nati Shalom, Cloudify

Cloudify CTO Nati Shalom added: "We are lowering the adoption barriers for NFV by leveraging open source software that accelerates VNF onboarding while reducing technology risk.

"Working with Proximus, we are deploying an NFV technology stack that is community-supported and interoperable with multiple cloud environments. As a result, Proximus will have better control of its destiny, costs and competitive advantage."

Proximus is also working with Cisco, F5, HPE, Palo AltoNetworks, Red Hat, Spirent and Tech Mahindra on the project. ■



JOHN LUND/GETTY

› *Large service providers continue NFV deployments, but questions remain*

Spoofing of Dutch politicians' emails raises heated debate over security flaws

Investigative reporters' revelations cause public controversy over journalists' responsibilities and the security practices applied to email servers in the Netherlands. Tijs Hofmans reports

The email addresses of Dutch politicians are easy to spoof, as journalists in the Netherlands showed in October 2017.

What followed was a heated debate about the responsibilities of reporters in revealing security flaws, and the implementation of common security practices on email servers.

The news broke after Dutch investigative journalists from Follow The Money (FTM), a website that specialises in financial news stories, posted an article about the possibility of spoofing emails sent in the name of Dutch MPs. Reporters found it was possible to send emails that appeared to come from @tweedekamer.nl, the domain used by the Netherlands parliament.

Flaw revealed

FTM worked with ethical hacker Maarten Boone, who tipped off reporters about the "leak". It was later revealed that Boone had been laid off by Fox-IT, a security company that advises the Dutch government on cyber security practices and which had revealed the flaw a long time ago.

To corroborate their story, the reporters sent several emails to Dutch MPs that were obviously fake, mostly concerning the then recently formed Dutch coalition. "Well guys, looks like we have to start talks all over again," a fake prime minister joked in a spoof email to other coalition partners.

The story attracted even more attention when popular Dutch TV show *RTL Late Night* showed some of the spoof emails during a national broadcast.

Framework lacking

The email spoofing is made possible by the lack of a sender policy framework (SPF) for the parliament's general network, a measure that is fairly easy to implement but is often glossed over by systems administrators. According to the reporters, sending an email in the name of Netherlands prime minister Mark Rutte would make a phishing campaign pretty effective.

Following the revelations, a heated debate broke out about the implications of the story, as well as the way it was framed. Many

Investigative reporters were able to send emails that appeared to come from the domain used by the Netherlands parliament

ALEKSANDARGEORGIEV/GETTY

security experts felt that Follow The Money had made a relatively minor problem seem much bigger.

But an SPF, although handy in such situations, is not the be-all and end-all solution to spoofing – a problem that can never be totally prevented. Using SPF, a domain can validate whether an email comes from the same domain or has been spoofed. In the case of the latter, usually the spoof email is immediately deleted or sent to a spam inbox. However, implementing an SPF sometimes raises the risk of marking too many false positives, resulting in unnecessarily deleted emails.

Other journalists and security researchers discovered more Dutch public authorities that had configured their email settings improperly. The Netherlands intelligence service AIVD, the national police force and several energy companies had not configured their servers properly, but did implement fixes several days after the story broke.

Many observers accused the reporters of making the news seem bigger than it really was. It was soon discovered that neither Follow The Money nor *RTL Late Night* had implemented the security measures they had criticised parliament for lacking.

There was also criticism about the impact of the "leak". Many pointed out that spoofing is difficult to prevent in email systems, and that common security practices – such as not clicking links on unexpected attachments – are always applicable, leading to claims that the story was not really news at all.

But a more serious accusation was that the journalists had not practised responsible disclosure, but went public with their findings immediately. The role of the media in responsible disclosure has always been a complicated topic, but it has been suggested that it is reasonable to expect even journalists to give a company some time to fix any bugs in its system.

Despite criticism of the journalists, several systems administrators were quick to implement security measures the same night that the story broke, apparently prompted by the publicity.

Urgent measures

In an update statement, the Dutch parliament said "urgent measures" had been taken to fix the vulnerability, which no longer exists. It also mentioned that "further steps" would be taken to double-check emails from non-secured domains, and to prevent future misuse of emails – but what these measures are remains to be seen.

Several other public bodies, including the intelligence services, also made fixes to their systems later that week, although several other domains remained vulnerable.

This is not the first time such security issues have been raised in the Netherlands. Several security experts have mentioned such discoveries before, but did not follow up on it because it seemed to be an unlikely-to-be-exploited problem that was difficult to prevent completely.

However, Labour MP Astrid Oosenbrug asked official questions in the Dutch parliament as long ago as 2015, and has done so several times since. According to reporters, the problem was well known among politicians but was not deemed important enough to take action.

> **"Politicians lack a sense of urgency in these matters"**
> Astrid Oosenbrug, Labour MP

"Politicians lack a sense of urgency in these matters," Oosenbrug was quoted by FTM as saying. She referred to an earlier incident when minister of economic affairs Henk Kamp was found to be using a private Gmail account to conduct government business. In the US, such a situation might have led to a candidate losing a presidential nomination, but reactions in the Netherlands were more tempered.

And this was not the first time the Dutch parliament's IT system had been compromised. Earlier in the year, a wave of ransomware encrypted files on MPs' computers after an infected Microsoft Word document was circulated. And in June, news website Binnenlands Bestuur found that almost all Dutch municipalities did not follow standard security practices for their email servers, making phishing campaigns easy to launch. ■

Educate users on ways to avoid email phishing attacks so you can rest easy

EU plan to collect biometrics of all visitors could include UK citizens after Brexit

European Parliament has approved entry/exit system covering all non-EU visitors to the EU, writes Jennifer Baker

The European Parliament has approved a new electronic system to store biometric information on all non-EU citizens travelling in and out of the bloc – and post-Brexit, this could include UK citizens.

The entry/exit system (EES) is part of the so-called Smart Borders package, and will consist of a central database storing the name, travel document, fingerprints, facial image, date and place of entry, exit and entry refusal of every third-country national – even visa-exempt travellers – coming to and from the EU Schengen area.

Data retained for three years

The data will be retained for at least three years – or five years for over-stayers – and will be accessible to border, visa and national enforcement authorities, as well as Europol, but not national asylum authorities.

The aim is to reduce irregular migration of over-stayers and fight organised crime, as well as speeding up border checks by replacing the manual stamping of passports. Data stored in the EES can be consulted to prevent, detect or investigate terrorist offences or other serious criminal offences.

Finnish MEP Jussi Halla-aho said: "Much of the data collected by the system could be vital in the fight against organised crime and terrorism. It is crucial that national police forces and Europol will now have access to the data."

But others have warned that such mass data collection is contrary to the EU Charter of Fundamental Rights and a recent court ruling. "A few months ago, the European Court of Justice rejected the EU passenger data agreement with Canada," said German MEP Cornelia Ernst.

That agreement envisaged storing similar data to the EES for up to five years. The court considered that holding on to such data for so long after the duration of a stay was an "interference with the fundamental right to respect for private life".

Ernst added: "We are against this mass data retention from travellers. It will cost millions of euros and is a shame for the EU."

French MEP Marie-Christine Vergiat said the scheme was originally intended to facilitate border crossing for the 50 million

third-country nationals who come to the EU each year. "However, this is now primarily a system for identifying people in irregular immigration situations and facilitating deportations," she said.

"Under the false pretence of security, Europe is multiplying repressive forces' access to sensitive data, including in cooperation with third countries like Sudan. Europe is turning into a bunker, undermining its own values and picking scapegoats for its problems rather than fulfilling our international responsibilities."

> **"Europe is turning into a bunker, undermining its own values and picking scapegoats for its problems rather than fulfilling our responsibilities"**
>
> Marie-Christine Vergiat, MEP

Tanja Fajon MEP, a negotiator for the new system, was also worried about the implications for "bona fide travellers who pose no threat to the EU" and who should "not be seen as potential terrorists". She added: "We need to keep the balance between the purpose of this system and fundamental rights."

The draft law had already been informally agreed with member states, and the European Commission is now pushing for it to be up and running "by 2020 at the latest". ■

The aim of the EU's biometric system is to reduce irregular migration of over-stayers and fight organised crime

BUDANATR/GETTY

Dutch digital coin miners offered space in datacentres to reduce electricity costs

The Netherlands' Datacenter Group has set up Crypto DC to provide digital coin miners in the country with workspace in a professional datacentre, writes Kim Loohuis

Digital coin miners can earn money by investing a few thousand euros in the right equipment, but electricity bills can eat into their profits.

Bitcoin is probably the best-known cryptocurrency, but there are many other digital coins, including Dash, Ethereum, Litecoin and Pure. After a spell mining Dash, Ko Hamer, a structural engineer at De Voogt Naval Architects, started mining Pure.

"Dash is an interesting coin, but it is getting tougher to be mined," he said. "Pure is a relatively new currency, with block rewards of about 100 coins. That is very interesting."

Earnings potential

Whether Hamer is going to get rich by Pure, he does not yet know. "I have earned about 2,500 coins a week over the last few weeks." he said. "If Pure is put on the Exchange for €50, I earned €1,250 a week. If it is not worth anything, I have lost €30."

Hamer began selling Antminer D3 machines last summer. The demand for these Chinese-made appliances is huge and while others couldn't get hold of any, Hamer managed to order 45 machines from supplier Bitmain. He kept two for himself and started mining cryptocurrency. "The downside of the machines is that they emit a lot of heat, make lots of noise and consume a lot of power," he said. "Because I live in an apartment, I have built an installation box, which reduced the noise level by 20 decibels."

The heat generated by the Antminer machine was not too much of a problem for Hamer – he used it to heat his house – but his energy bill shot up.

Digiconomist has estimated that mining the popular Ethereum currency globally consumes more than 4.5TWh of electricity each year, which is almost as much as a country like Moldova – with a population of about three million – uses annually. The mining of bitcoin uses considerably more power – 15TWh a year, which is enough to light the Eiffel Tower for 250 years.

All this power costs a lot of money, which reduces the profits of digital coin miners. To maintain their profitability, miners need their energy resources to be as cheap as possible.

In Iceland, a "bitcoin mine", based on the country's relatively cheap geothermal energy, has been set up. Similar mines have also been created in China and the US, where they get their energy from water or solar power. And in northern Sweden, which also has cheap energy, a large datacentre was established for mining cryptocurrencies last summer.

In the Netherlands, Hamer got into contact with Crypto DC, part of the Datacenter Group, which offers digital coin miners access to professional datacentre facilities.

"Miners do not have to deal with a large datacentre directly – we do it for them," said Daan Posthuma, Crypto DC's initiator. "Through our agreement with the Datacenter Group, we can provide miners with low energy prices."

Special lower rates

Hamer added: "Because a datacentre uses a lot of energy, it can command special lower rates with the supplier." Other advantages are temperature and humidity, said Hamer, who has now placed his Antminer machines in the Crypto DC datacentre.

Miners can use a special portal to log into their machines remotely, said Hamer. "That way, I can check if my miner is doing well or I can switch to another pool or currency if I want to."

Datacentres are often too expensive for regular digital coin miners or their contracts are too long-term, so Crypto DC negotiated special rates with the Datacenter Group. "We offer an all-in-one price for the rack, power and internet connection," said Posthuma.

Hamer is happy about moving to a professional datacentre. "Even if it is more expensive, a datacentre is still a better environment for your machine than at home," he said. "The air in a datacentre is better, which is important for the life of your machines. And with the all-in-one price, you know exactly what to expect."

Cryptocurrency mining is gaining popularity in the Netherlands, judging by the wide range of new and second-hand machines on Marktplaats (a Dutch digital marketplace, much like eBay). Demand for graphics cards has also risen sharply.

> **"It's unfortunate that more and more people know about this. If they didn't, we miners could become rich while we sleep"**
> Ko Hamer, De Voogt Naval Architects

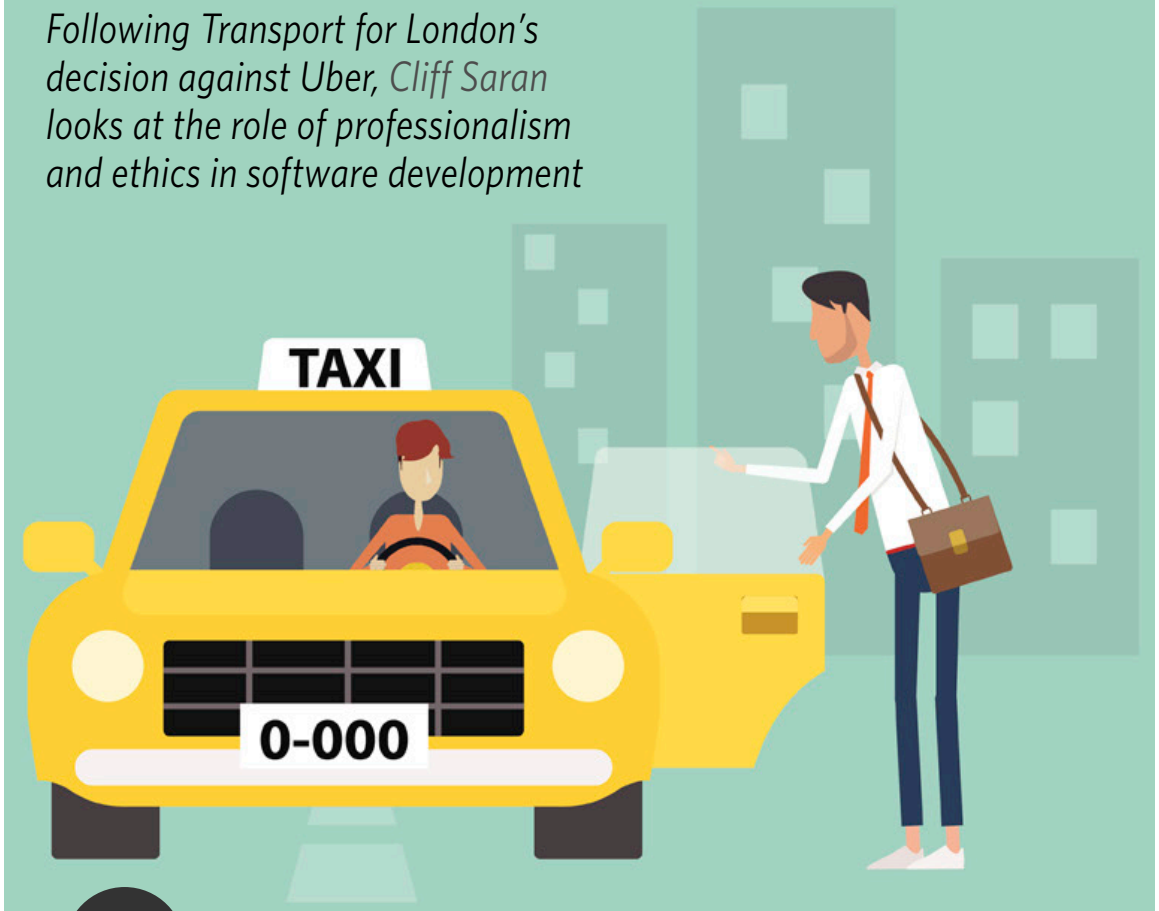
As more and more people take up digital currency mining, it is becoming more difficult to do so successfully. Posthuma said there will come a time when mining is no longer attractive for people at home because it will become too expensive. "As long as people can buy equipment and pay their energy bills, they can continue, but somewhere there will be a tipping point when only mining in a professional environment will be attractive."

Hamer added: "Sometimes it's quite unfortunate that more and more people know about this. If they didn't, we miners could become rich while we sleep." ■

Why have digital currencies yet to reach the mainstream market?

Uber, Volkswagen and the ethics of software

Following Transport for London's decision against Uber, Cliff Saran looks at the role of professionalism and ethics in software development



TCMAKE_PHOTO/GETTY

Uber was the latest company to get caught out for using software to help it overcome official audits and tests. Among the reasons Transport for London (TfL) gave in September 2017 for not renewing Uber's licence to operate in London was the software that the app-based taxi firm allegedly developed to avoid officials inspecting its drivers.

While newspaper commentary was largely about the Licensed Taxi Drivers' Association, which represents London's black cab drivers, lobbying TfL against Uber, an important part of its decision was Uber's stealth software.

This is not the first time a company has been found to have written software explicitly to get around official tests and audits.

Volkswagen's admission

In May 2014, Volkswagen was found to have modified its engine management software to detect when diesel cars were being run on an official emissions test, so it could dial down the emissions. The car maker effectively wrote software specifically to cheat, according to the *New York Times*, which wrote: "Volkswagen admitted 11 million of its vehicles were equipped with software that was used to cheat on emissions tests."

The newspaper reported that an on-road test conducted by West Virginia University found some cars emitted almost 40 times the permitted levels of nitrogen oxide. This led to the California Air Resources Board's investigation of Volkswagen.

Looking at TfL's decision not to renew Uber's licence to operate in London, among its concerns was the use of so-called Greyball software, which geofences government and official buildings.

HOME

The software reportedly presents an alternative site to customers, or people wishing to book a ride from outside those buildings, which is used to prevent officials from booking an Uber ride.

Other cities have been concerned abut the use of Greyball software. In a blog post, Gerald Gouriet and Charles Holland of barristers' chambers Francis Taylor Building described Uber's Greyball program as a way to identify regulatory staff using the customer app and thereby avoiding regulatory activity, and highlighted the case of New York. "Uber initially robustly defended the program, but after six days, announced it would be withdrawn," the pair wrote.

The US City of Portland recently published an audit looking into the use of Greyball software at Uber, which confirmed that the transport company had admitted using such software. "In a letter dated 21 April 2017, Uber's counsel provided their second response. In this response, the company admits to having used the Greyball software in Portland for a two-week period, from 5 December to 19 December 2014 against 17 individual rider accounts," the audit report said.

> *Many experts have warned of the potential for the digital revolution to cause social and cultural unrest. Have we reached a tipping point?*

Evade regulators

The records provided by Uber show three of those individual riders actively requested and were denied rides on the Uber platform, the court filing stated. The company said it would never engage in a similar effort to evade regulators in the future.

But as Computer Weekly's sister title, TheServerSide, notes, the company's record of unethical practices in software development appears to reveal a culture of contempt among managers. On her blog about sexual harassment at Uber, Susan Fowler wrote about a "toxic culture" in the company, where managers refuse to cooperate. "I remember a very disturbing team meeting in which one of the directors boasted to our team that he had withheld business-critical information from one of the executives so he could curry favour with another," she wrote.

There is also the case of Uber's God View tool, infringing users' privacy by collecting data about their location even when the Uber app is not being used.

Overcharging clients

Beyond Uber and Volkswagen, examples of unethical coding include overcharging clients, producing poor quality code, and stealing intellectual property.

In a post on open source repository GitHub, one developer has been trying to raise the profile of coding ethics. The developer described how on one occasion, an employer asked to change the value of refund vouchers on an e-commerce site to make the refund worth less.

The coder wrote: "I think we need to establish a code of ethics for programmers. Doctors, social workers and even lawyers have a code of ethics, with tangible consequences for skimping on them. Why not programmers as well?

"I want to live in a world where a programmer who hasn't agreed to follow our code of ethics has a hard time getting employed. It

is simply not acceptable to write code that is harmful to users. What the hell is wrong with these people?"

The Association for Computer Machinery's ethics statement says: "Software engineers shall approve software only if they have a well-founded belief that it is safe, meets specifications, passes appropriate tests, and does not diminish quality of life, diminish privacy or harm the environment. The ultimate effect of the work should be to the public good."

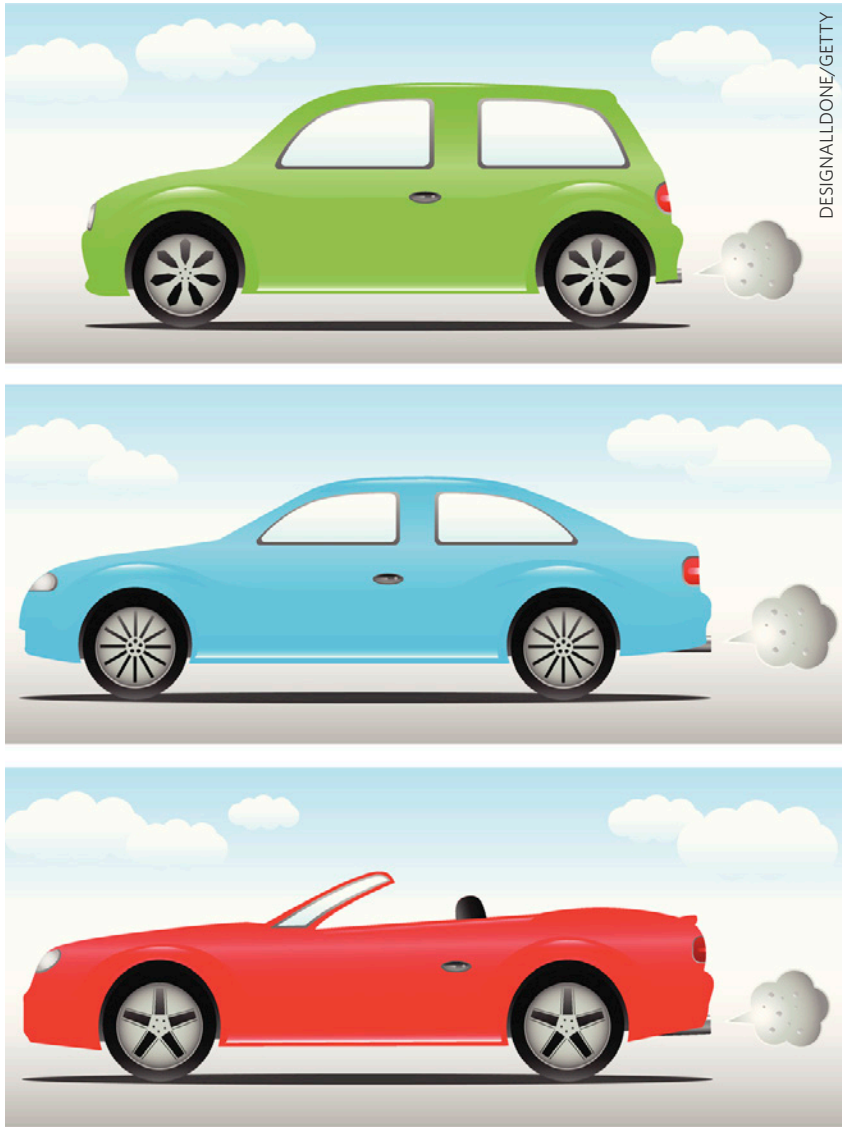
Ethics in software engineering is also an area that has been looked into by the BCS, The Chartered Institute for IT. The BCS's code of conduct for its members: "You shall have due regard for public health, privacy, security and wellbeing of others and the environment."

Improve human wellbeing

David Evans, BCS director of policy and community, believes an overriding outcome in the domain of computing should be to benefit society and improve human wellbeing. For organisations that value customer relationships, ethics is very important, he says: "In the academic world, ethics is top of the checklist."

But working in an ethical manner can be challenging. "The idea of public benefit or human wellbeing turns ethics into a misplaced concept," says Evans. "You can lose the reason why you do it. We want professionals who do things that do not cause harm to others, and we also want our IT team to understand the effects of what they do."

The value of working ethically should, says Evans, be ingrained into corporate culture, including IT and software development.



DESIGNALLDONE/GETTY

He says organisations will benefit if IT understands the human impact of what it does.

The challenge for people working in IT is that the impact of their work can be quite abstract, says Evans. "It is hard enough to think about what is illegal. It's harder to get people to understand how their work will impact other people," he says.

Drive new opportunities

A case in point is the Data Protection Act. A business may want to use its customers' data in certain ways to drive new opportunities. "I have seen reputable companies celebrating tech success when their developments are in breach of the Data Protection Act," says Evans. "Ethics may constrain you from doing things that may make money." He argues that data sharing is not an ethical question: "It is the actual law."

For the BCS, ethics goes hand-in-hand with professionalism. The software industry appears to operate without much regard to the impact on individuals and businesses, says Evans. "A construction company cannot build a huge dam without consultation," he says.

"We will need this in software, but the problem with Silicon Valley is that a small startup in a bedroom can disrupt major industries around the world. Dialogue becomes necessary."

> **"The problem with Silicon Valley is that a small startup in a bedroom can disrupt major industries around the world. Dialogue becomes necessary"**
>
> David Evans, BCS

The industry is now entering the dawn of machine learning, where artificial intelligence (AI) is used to process vast amounts of personal data and then make decisions without the vagaries of human decision-making.

Ethics, as it relates to AI, was among the topics that author, broadcaster and tech philosopher Tom Chatfield spoke about at the InterSystems Technology Summit in October.

"We are busy translating the fabric of our societies into something machine-readable; into data on a scale that only machines can handle, and that, in turn, will fuel the next generation of machine learning," he says.

Walker says there are two points to consider as the world moves more into the digital domain: the quality of the translation, and its capacity for iteration and improvement.

"The exponentially increasing volumes of data handled by our tools can, when used well, feed the actionable small data and intuitive insights human lives thrive upon – but they can also create a locked-down world in which decisions occur beyond our scrutiny," he says.

For Walker, this is the difference between tools that can make integrated health records available anywhere, at the touch of a button, and tools that deny someone insurance based on an inscrutable algorithmic reading of their life. ■