HUNTING FOR SPIES IN COMPUTER CHIPS

Becoming a Max Planck Director via "second-chance" education is probably something of an exception. But that is precisely what happened in the case of Christof Paar, one of the founders of the Max Planck Institute for Security and Privacy in Bochum, where his work now includes tracking down hardware Trojans on computer chips.

TEXT: KLAUS JACOB

Christof Paar has fond memories of the construction of the Colonius telecommunications tower in Cologne. In 1980, the soaring stairwell that provides access for the fire service had to be fitted with loudspeakers: four of them at every ten meters of height. This laborious task fell to an apprentice in his first year – namely, to Christof Paar. Since then, the former telecommunications technician has climbed to the upper echelons of science to become one of the founding Directors of the Max Planck Institute for Security and Privacy in Bochum. His research work at the Institute is also of great political relevance – and he's a good contact when it comes to Huawei and 5G networks or the protection of companies against hackers.

When you look at the individual milestones on Christof Paar's résumé, it is clear that his journey to becoming a Max Planck Director is something of a rags-to-riches story. In the beginning, things didn't look all that promising. While attending an academic-track high school, Paar struggled with languages and therefore switched to an intermediate secondary school, where he obtained his "Mittlere Reife" diploma. He then went on to complete an apprenticeship, but it doesn't sound as if he regrets going into a skilled trade – indeed, he says that, even as a young boy, he enjoyed tinkering with things and was fascinated by technology. His parents were actually quite accepting of his decision to learn a trade, even though his father was an academic. Having qualified as a tradesman, Paar then took something of a roundabout route into the world of science. After all, switching from a skilled trade to an academic career was harder in those days – almost 40 years ago – than it is today. Paar first attended a specialized upper secondary school. He graduated after one year and then spent half a year working as a journeyman at a small three-man firm. "I used to ride my motorbike to the building sites." He then pondered "for weeks", whether to become a master craftsman or switch to studying for a degree. His boss urged him to stay, taking the view that a career as a master craftsman offered much more security than becoming an engineer. In the end, Paar opted for the academic route and signed up to study telecommunications at Cologne University of Applied Sciences. "It was a rational decision," he says, adding that the higher earning potential was the decisive factor.

On his detour through so-called "second-chance education", Paar managed to fulfill many of the expectations one has of a Director of a Max Planck Institute: his excellent academic performance was impressive, not least because he was – and still is – enthusiastic about his subject. His eyes light up when he talks about fast microprocessors or the fight against hackers. The 57-year-old Director is talkative, easy to get along with and full of laughter, and takes a relaxed approach to team meetings. Although most of his team members are young researchers, Paar treats them as equals; he is open to criticism, and is on familiar terms with everyone.

→

VISIT TO

CHRISTOF PAAR

PHOTO: LARA WITTHAUT, FOTO-OSTERMANN.DE FOR MPG

A passion for technology: Christof Paar hunts for security flaws in computer hardware.

PHOTO: LARA WITTHAUT, FOTO-OSTERMANN.DE FOR MPG

Youthful and fit: it's no surprise that Christof Paar is in such good shape, especially thanks to his tri-weekly karate training sessions.

Meetings with Paar have a relaxed, collegiate atmosphere – with pizza and coffee at the ready. Indeed, Paar looks much younger than his years, partly thanks to his lean physique. Thrice-weekly karate sessions help him to keep fit.

Paar graduated from Cologne University of Applied Sciences at the top of his class – and was one of only a handful of graduates to complete the degree within the prescribed period of study. He met a group of fellow students who spurred each other on to high achievements. "The A-Team," he says with a smile. It was in those early days, while working as a teaching assistant for math, that he discovered his passion and talent for teaching. For his dissertation, he developed an electronic control system for flip-disk displays such as those on buses, where the names of the respective stops are displayed by an array of tiny disks that flip to show either their black or white side. To this day, a large display of the same type notifies traders of current prices at the Frankfurt Stock Exchange. The technology, which was very advanced in those days, is known as an "embedded system" – in other words, a combination of a computer and a physical device. This is the area of research that Paar still works on today – and even then, at the age of 24, he knew exactly what he wanted his future career to look like. "I wanted to become a professor, without a shadow of a doubt." Indeed, his main motivation in those days was teaching.

Of course, this meant that he would first have to do a doctorate, which wasn't possible at a university of applied sciences in those days. So with that, together with the A-Team, he switched to the University of Siegen, where he was largely spared the need to complete the basic course of studies. However, as an acknowledged conscientious objector, he first had to complete his civil service as substitute for the compulsory military service – and he was in luck: the audiologist Hasso von Wedel, who had made a name for himself as a tinnitus researcher, was offering two research-related positions for conscientious objectors at the University Hospital of Cologne. Paar secured one of the posi-

tions and was responsible for the technology used in the experiments. As a result, he actually managed to turn this forced career break to his advantage. During his civil service, he attended lectures in physics and mathematics at the University of Cologne, and toward the end he began his studies at the University of Siegen.

From Siegen, he moved to the U.S. to write his second thesis – at Michigan Technological University. But why would someone who had to switch schools because he struggled with foreign languages move to the U.S.? "Of course, my thirst for adventure was a key factor," says Paar. Moreover, he had already hitchhiked across the U.S. twice during his time at Cologne University of Applied Sciences, and had found it much easier to learn the language by conversing with Americans than he did in school. He even went on to marry an American woman. "My English teacher would be pretty amazed," he laughs.

Paar spent a long, cold winter in Michigan working on his Master's thesis. Once again, he chose a topic that was at the cutting edge of technical development: active noise cancellation, a technology that is intended for use in cars, for example; it cancels out undesired noise using what is colloquially known as "anti-noise." Paar has a habit of combining different fields within his projects: physics with computer technology, engineering with mathematics, classical hardware with software. His doctoral thesis at the University of Essen is another example. This time, his focus was on error correction in digital technology – a technology that is used in data transmission from satellites to Earth or in CD players, for example. Very few people who listen to a CD are aware of the sophisticated mechanisms that operate in the background to ensure that even scratched CDs can be played without errors. The technology even makes it possible to drill a hole with a diameter of up to three millimeters into the disk without affecting playback. Paar simplified the algorithms for real-time error correction, which are implemented directly in the form of special hardware circuits, in order to make them significantly smaller, faster and more energy-efficient – a method that was later put to commercial use.

After completing his doctorate, Paar planned to embark on an academic career in the U.S. so that he could be with his girlfriend, whom he had met two years earlier and later married. "Two years of long-distance relationship were enough." In 1995, he was offered a position as assistant professor at Worcester Polytechnic Institute in Massachusetts, a private university that is funded by tuition fees and therefore places a lot of value on high-quality teaching. As part of the application process, Paar was required to deliver not only a research lecture, but a teaching lecture as well – and with that he outdid his competitors. The freedom he now enjoyed as a professor allowed him to introduce a new subject at the university: cryptography.

Paar works on the implementation of new encryption methods in hardware and software. He is one of the experts who established this area of research.

The word cryptography conjures up images of the secret codes that children find so fascinating, or of the Enigma, the Nazi encryption device whose code was cracked by the Allies. As a research discipline, however, cryptography still led a marginal existence in the 1990s. There was only a single textbook, which was brand new at the time – and the subject was only offered at a few universities. Paar had backed the right horse. "Luck was also on my side," he says. Back then, the rapid expansion

→

of the dot-com bubble was making cryptography and data security increasingly important. Their importance has also been bolstered by cases such as that of the whistleblower Edward Snowden, who revealed just how brazenly intelligent agencies intercept data and how important it is to protect them. Another of the countless examples is the scandal surrounding Crypto AG, a Swiss company that manufactured encryption devices during the Cold War. It later emerged that the company had been selling manipulated devices on behalf of the CIA and the German Federal Intelligence Service (BND), allowing the secret services to conduct espionage in over 100 countries.

However, Paar's work doesn't focus primarily on the development of new encryption methods, but rather on their implementation in hardware and software. Indeed, he is one of the experts who established this area of research within the scientific community.

he returned to Germany – partly to be closer to his elderly parents, but also for the opportunity to help establish the Horst Görtz Institute for IT Security at the Ruhr University in Bochum. The initiative for founding the Institute came from Horst Görtz, the owner of a medium-sized business who made his fortune in IT security during the dot-com boom. It was born of his desire to use his foundation to launch an influential research institute in Germany. Paar's two older children, Noah and Maja, found the move to Germany easy – they had been raised bilingually and entered elementary school here, while his younger daughter, Flora, was born in Germany. For Paar's wife, the transition was more challenging from a career perspective. In the U.S., she had taught at a community college – a type of higher education that doesn't exist in Germany. She now works as a lecturer in biology at the Ruhr University in Bochum. "The job brings her a lot of satisfaction," says Christof Paar.

Subtly manipulating just a few transistors is often enough to deactivate vital safety functions.

Together with his colleague Çetin Koç, he launched the Conference on Cryptographic Hardware and Embedded Systems (CHES) in 1999. Although the conference was actually intended to be a relatively small workshop, the first CHES was attended by over 150 international specialists from academia and industry and was even covered in the New York Times. Today, CHES has evolved into one of the most important international conferences in the field of cryptography.

But let's turn our attention back to Christof Paar's journey from a mere apprentice to becoming a Max Planck Director. Paar stayed in the U.S. for seven years, during which he rejected a number of offers to join start-ups – because he enjoyed university life and the combination of research and teaching that it offered him. He was also worried that getting involved in a start-up would mean he would no longer have enough time for his wife and children. In 2001,

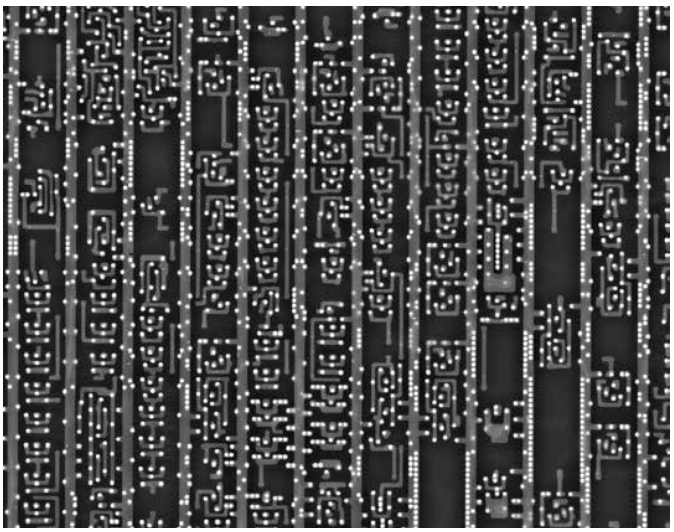
In any case, things are going well for him: not least thanks to the Horst Görtz Institute, Bochum is now one of the world's leading locations for IT security and is home to 1,000 students in the field. However, the Institute has caused a stir not only within the scientific community – in 2008, Paar and his colleagues succeeded in cracking the security system used in an electronic door opener that controls millions of car and garage doors. To do this, the researchers first had to analyze the electronics using a very laborious process known as reverse engineering. The resulting insights allowed them to produce a sort of master key that could open garage doors and the doors of some cars. This was a major story for the media. "We were overrun by journalists for weeks," says Paar.

Such "vulnerability research" projects like these are part of Paar's everyday work – after all, those who seek to improve security need to be aware of a

→

PHOTO: LARA WITTHAUT, FOTO-OSTERMANN.DE FOR MPG

Secure monitoring: Christof Paar's team is developing technology that can be used to check whether nuclear warheads are stored securely. The monitoring cannot be circumvented, because the warheads record an electromagnetic signature that is specific to the storage site. It is this connection to physical characteristics that links the project to research into computer hardware.



GRAPHIC: KRIMINALTECHNISCHES INSTITUT DES BKA - KT 52

Scanning components: this image from a scanning tunneling microscope reveals details in the chip structure that help the researchers in Bochum to search for hardware Trojans.

system's weaknesses. But Paar goes one step further: he also wants to know what makes hackers tick, what their thought processes are, and where their mental restrictions lie. This has led him to develop a new area of research in collaboration with Nikol Rummel, a cognitive psychologist at Ruhr University Bochum. The two researchers were confronted with a problem: professional hackers are reticent. They keep their cards close to their chest, even when working for companies that have hired them to seek out vulnerabilities in their products. Paar and Rummel had to make do with students from Ruhr University who volunteered to participate. Through this research, they discovered that the speed at which a hacker makes progress is correlated with the hacker's working memory. From cognitive psychology, we know that most people can process a maximum of seven units of information at the same time. One approach to preventing hacking attacks is therefore to design hardware and software so that attackers have to grapple with significantly more information. Christof Paar and the French researcher Gilles Barthe became the founding Directors of the new Max Planck Institute in Bochum in 2019. Now, Paar can spend more of his time on research – for which he also works with the Federal Criminal Police Office, or BKA, and companies such as Google. That being said, he doesn't want to give up on teaching altogether. "The difference is that, now, I can cherry-pick the most interesting topics," he says. A highlight is Paar's introductory lecture on cryptography that he successfully introduced in the U.S., albeit in an updated form.

The current wrangling over Huawei highlights the importance of Paar's research area. The U.S. and Britain suspect the company of spying for the Chinese state and are excluding it from the rollout of 5G technology. Paar is all too aware that manipulations of this kind are possible. After all, he also studies hardware Trojans – and he has received an ERC Advanced Grant on this very topic, one of Europe's most prestigious research awards. Hardware Trojans – in other words, circuit manipulation within a computer chip – can be used for espionage and could even allow attackers to shut down entire industrial systems.

Non specialists could be forgiven for thinking that manipulation of this kind can't be too hard to find – but they would be mistaken. Chips such as those inside smartphones or in 5G-connected computers contain many millions of transistors that measure just a few nanometers across and whose schematics are a carefully guarded secret. Christof Paar and his team have found that subtly manipulating just a few of these transistors is often enough to deactivate vital safety functions. To understand circuits of this kind, the researchers must laboriously analyze the chips layer by layer, with the help of ablation techniques. Meanwhile, they have developed an automated method for analyzing the high-level structure of the computer chip. For example, this allows them to identify the sub-modules of the chip in which encryption takes place – sections that are especially suited for introducing Trojans. Until now, these analysis techniques were only available to powerful intelligence agencies and a small number of specialized firms. However, Paar's research will help the entire international research community gain a better understanding of hardware manipulation, so that new safeguards can be developed.

Exactly how attacks by governmental or semi-governmental organizations can be foiled is the subject of research at the Cluster of Excellence "Cyber Security in the Age of Large-Scale Adversaries" (CASA), of which Christof Paar is one of the speakers. "As we know from Edward Snowden's revelations, intelligence services sometimes go to absurd lengths to circumvent security solutions," says Paar. It seems unlikely that he will run out of work anytime soon.

Hermann Neuhaus's

Hermann Neuhaus Prize

FORWARD.
VISION.
FUTURE.

€ 25,000

Apply until
February 15th, 2021

The Hermann Neuhaus Prize recognizes excellent postdocs and group leaders in the Biology & Medicine Section **(BMS)** and the Chemistry, Physics & Technology Section **(CPTS)**. The prize enables the successful applicant to develop her or his research's potential for application.

For more information visit
www.mpg.de/hermann-neuhaus-prize