Spies in the Service of Security

From e-mailing to online banking, the things we do on our computers on a daily basis are fraught with risks. Dealing with these kinds of security vulnerabilities is the domain of **Michael Backes**, a fellow at the **Max Planck Institute for Software Systems** in Saarbrücken. The methods he and his team employ are surprising, to say the least.

TEXT **TIM SCHRÖDER**

Photo: MPI of Computer Science – Hardy Müller

Greetings from James Bond: Michael Backes and his team employ unconventional methods to get to the bottom of perceived security vulnerabilities in our electronically shaped world. The computer scientists' projects include reconstructing the content of printed texts from recordings of printer noise, and using a telescope to decipher the computer monitor content reflected in, for instance, a glass teapot (pp. 74/75).

For the ordinary mortals among us, trying to comprehend what Michael Backes does at work every day is way beyond our capacity. Backes, by contrast, understands even the deepest depths of the mathematics behind it, the convoluted paths that lead through a world of abstracts. Backes is a computer scientist. He is 33 years old and, at the age of 26, was Germany's youngest professor. He tinkers with mathematical proofs, logical consequences and complicated if-then rules where an assumption holds true if X is an element of a certain subset or if sigma has the attribute H.

Michael Backes is professor of information security and cryptography at Saarland University, as well as a fellow at the Max Planck Institute for Software Systems in Saarbrücken. He likes puzzling over things that most people consider secure. "When someone develops a new encryption technique, I think 'great,' and then I try to break it." Backes roots around for security flaws in the high-tech aspects of our everyday life, for data loopholes that no one has yet noticed. And he tries to stop the gaps with better security plugs.

One particular method has been on Backes' mind a lot in recent months: zero-knowledge proof, a mathematical proof method. It is one of those old ideas that grab people's interest but then disappear into obscurity when it turns out they're completely impractical in everyday life. Backes has dragged zero-knowledge proof back out of the closet, dusted it off and used it to embark on a new chapter in Internet security. Zero-knowledge proof may be abstract, but it has what it takes to free Internet users from the burden of passwords once and for all: sender and recipient recognize each other without the need for any cryptic combinations of letters and numbers.

Zero-knowledge proof is a paradoxical thing. The name itself says it all: proving something without giving anything away. How is that supposed to work? Zero knowledge – really? Michael Backes offers an example: Imagine a treasure hunter who finds an ancient shipwreck filled with a hoard of gold. He then needs to find a financial backer who can raise the ship for him, but he doesn't want to give away the secret of where the find is located. So he brings a few coins or a piece of the wreck with him as proof. "The analogy doesn't quite hit the mark," admits Backes. "If it was a real zero-knowledge proof, the treasure hunter wouldn't even have to show the coins to prove he knew the site of the find."

TRUSTWORTHINESS – A MATHEMATICAL MATTER

It's a bit like that for all of us these days, with the constant need to prove that we are ourselves on the Internet – typing in passwords to access our bank accounts or entering credit card numbers to do our online shopping. Quite a few of us harbor silent fears that there may be someone sitting out there somewhere, capturing the data and hacking into our PIN numbers. Many people consider the modern-day Internet to be untrustworthy, as lawless as the streets of Chicago during Prohibition.

There is a great desire for more security, and that is exactly what Backes' zero-knowledge-proof ideas may be able to offer. The method uses mathematical means to verify whether information is reliable. It is based on the requirement that the user possess a trustworthy data document that guarantees authenticity – an electronic ID card, for example, that provides reliable information about whether the user is over 18. The zero-knowledge proof then acts as a sort of mathematical interface. It tells the recipient that the sender's data, such as his or her age, is correct. But it doesn't reveal the date of birth. From the mathematical codes, the recipient's computer can then determine whether the sender belongs to a group of trustworthy people. Of course the recipient doesn't get to know who the sender is – the sender's anonymity remains intact.

Anyone who wants to download a horror movie from an online video service must prove they are over 18. To do that, they have to specify their date of birth or other personal data – just the sort of information that is not particularly safe in the world of the Internet. The zero-knowledge-proof method, however, works without the date of birth because all it does is prove, using mathematical rules, that the person is over 18.

As incredible as it may sound, it really does work. Zero-knowledge proof was developed in the 1980s. And it does indeed enable the verification that a sender is trustworthy and that a statement is true. However, the mathematical communication between sender and recipient is complex and much too slow for the lightning-fast Internet. So it comes as no surprise that the method fell into a deep and extended sleep.

For some time now, there have been ideas on how it might be possible to develop more practical solutions. Backes is building on these to develop new and simplified Internet protocols, little send and receive programs based on zero-knowledge proof. For years, no one was able to verify, within a reasonable timeframe, how safe these offshoots of zero-knowledge proof actually were. But Michael Backes did it. He developed a software that can calculate in seconds whether a protocol is indeed watertight. This paves the way for the good old zero-

knowledge-proof idea to make its way into the Internet. What's more, he and his team developed a kind of mathematical black box to hold an Internet user's confidential details, such as data from an ID card.

The box can provide selective answers depending on the type of query, such as the age of the person concerned – without, however, giving out the confidential data itself. Rather, it is the memory that the zero-knowledge-proof machinery accesses in order to prove that the data is correct. In real life, if you want to prove your true identity to someone without revealing any confidential information, you go to a notary. The notary verifies the data on your ID card and confirms to the interested party that you are who you say you are. In a safe Internet of the future, the zero-knowledge-proof method could do the job of the notary. And no one would ever have to remember a password again.

As a fellow of the Max Planck Society, Backes, together with his team, can carry out his research freely. He works at a high level of abstraction, and there are people who openly call him a genius. But his work is by no means so up-in-the-clouds as to be out of touch with reality. It is practice oriented. "That's why I became an IT-security researcher," he says. "I wanted to work my way into a discipline in which people can still understand what I do."

Backes completed his undergraduate studies in just two semesters; one year later he was already at the point of choosing the subject for his thesis. He opted for IT security, a subject about which he is still enthusiastic today. "When it comes to security, we always make certain assumptions – about the hacker who dials in through the data line, for example. And then we construct a countermeasure to prevent it. But where it gets really exciting is when you push the assumptions to one side and a whole new range of threats become conceivable," says Backes.

THE PUPIL AS A BEARER OF SECRETS

At least once a year, Backes allows himself the luxury of taking this thought to extremes and investigating threats that he normally has nothing to do with, and that no one else has even noticed before. That's how he came up with the idea of photographing the images on computer monitors from a distance using a strong telescope and a camera. This would have been nothing to write home about if Backes and his team had taken pictures of the computer screens directly. But monitors are usually positioned with their backs to the windows. That was something Backes had noticed when walking to the cafeteria, and whenever he glanced into the offices of his fellow scientists. Then the idea hit him: Surely it must be possible to photograph the image on a monitor as reflected in any mirrored surfaces in the office? The results were impressive. Almost any shiny object in the room reflects the image from the computer practically straight out the window. The absolute top reflector was a glass teapot. On its curved surface, the scientists from Saarbrücken could even read a mirror image of text written in 12-point font from a distance of ten meters – using equipment that cost all of 1,200 euros: a digital camera, two telescopes and a bit of image analysis software. Eyeglasses and even the pupil of the computer user's own eye are sufficiently reflective for this purpose. Fellow scientists from the institute and the university helped Backes analyze the images.

"Hacking into the security systems of government agencies, private companies or scientific labs is way too time consuming these days," says Backes. So data thieves are becoming creative and inventing new tools with which to do their spying. And so is Backes. "How do you steal confidential patient information?" is a question he recently asked himself – and one that landed him the spying coup of 2009. "Not necessarily by trying to tap into the data line." He and his team pondered the question together in the office for a while and came to the conclusion that printer noise was the key. >

Photo: MPI of Computer Science

When doctors in Germany print their patients' prescriptions, they must use dot-matrix printers. This is because, unlike inkjet printers, they can be used to make carbon copies. The team in Saarbrücken wondered whether it would be possible to work out which words were being printed simply by listening to the kind of printer noise that has been pouring out of the dot-matrix printers completely unfiltered for decades. First the scientists tried to make out individual letters in the jumble of noise, but they were all blurred in the din.

Then they changed tack and tried to listen for whole words. They started by printing out single words on a dot-matrix printer, recording the sound of each one and using it to teach a sound-analyzing program. Following this, they played the computer recordings of short texts on a range of subjects – an article from Wikipedia on computer technology, one on Barack Obama and one on architecture. And believe it or not, the computer recognized 65 to 70 percent of the words correctly. That was enough to understand what the text was about.

Then they decided to put it into practice. Backes spoke to a medical practice in Saarbrücken, installed a miniature radio microphone under the printer, and sat down in the waiting room with a laptop. Whenever the printer made a sound, the laptop recorded the acoustic stream. Despite the background noise, conversations at the desk or talking on the phone, the sound-recognition software cleanly pulled words and numbers out of the carpet of noise – even recognizing abbreviations such as "pills for sore thr." without a hitch.

New ways of stealing data – that's what gets Backes' pulse racing. He wanted to know how great the threat actually was, so he started taking a survey among doctors, and at banks, too, as they also still print account statements and other documents with dot-matrix printers. "The results came as a complete surprise to us: 60 percent of all medical practices and 30 percent of banks still use dot-matrix printers today, and not one of them has paid a bit of attention to the acoustic emissions," says the computer scientist.

Michael Backes thinks best when he's out walking. He gets more out of meeting friends at a café or bar than sitting in front of his computer for hours. Perhaps that's the secret to his success. After all, what he has accomplished and the distinctions he has achieved are things that take others decades to attain. In 2009, the science magazine Technology Review, published by the renowned Massachusetts Institute of Technology, named him one of the "TR35," the world's 35 best young scientists, the ones who are going to change the world. No other German has previously been given this honor.

INTIMATE DETAILS ON THE INTERNET FOR ETERNITY

Admittedly, this success stems partly from the fact that Backes works with such a mass medium as the Internet. It is a medium that concerns every last one of us; we are all affected by its security, or lack thereof. Anyone who puts his or her private data or intimate details on the Internet must understand that the information will be perpetuated for all eternity and thus impossible to erase. The Internet can easily turn into the modern equivalent of being branded forever. But what counts as intimate details? And what or how much can I give away about myself and still retain my anonymity? These are also among the things Backes thinks about.

"It's amazing how quickly you can work out an Internet user's personal profile from tiny fragments, from fairly harmless information," says the scientist. There have long been software programs available that compare the concordance of various bits of information. The method, known as matching, is a way to compile pieces of data that fit a common profile – of one and the same person. If someone rates adult movies anonymously in an Internet forum, you might think that would be as far as it went. But if they discuss some of the movies non-anonymously in another – public – forum, a matching program can spot the similarities and assign the anonymous data to that person. "These matching tools are starting to become powerful enough to plow through the enormous quantities of data on the Internet in a truly systematic manner," says Michael Backes, "and there is a danger that personal data may start to be used and exploited to a much greater degree." That's why he's attempting to assess the loss of privacy. "How anonymous am I after entering certain information on the Internet?" he ponders. Backes is developing programs, called protocols, that are capable of correctly gauging the privacy loss.

After completing his computer science studies, Backes' first job was at IBM's research lab in Rüschlikon, Switzerland, where he worked on security systems. Then Saarland University gave him a lifetime appointment as a professor. That was more than six years ago. Given the pace at which Backes has been moving thus far, it should be fascinating to see what's next. And who knows – he may already have a fan club out there, waiting with bated breath for the next espionage highlight of the year. ◀

GLOSSARY

Cryptography
Even in ancient Egypt, cryptographic methods were used to encode information. The word comes from the Greek and means "secret writing." These days, cryptography is mostly concerned with information security – in other words, designing, defining and constructing systems that can prevent unauthorized reading and modification.

Matching
In cryptography, matching is the search for concordance between various pieces of information. A software program designed for matching can, for example, detect similarities and match anonymous data to a certain person.

Zero-knowledge proof
A method in which two parties (the prover and the verifier) communicate with each other. The prover convinces the verifier with a certain level of probability that the prover knows a secret, without giving away any information about the secret itself. The prover and the verifier exchange mathematical codes to achieve this.