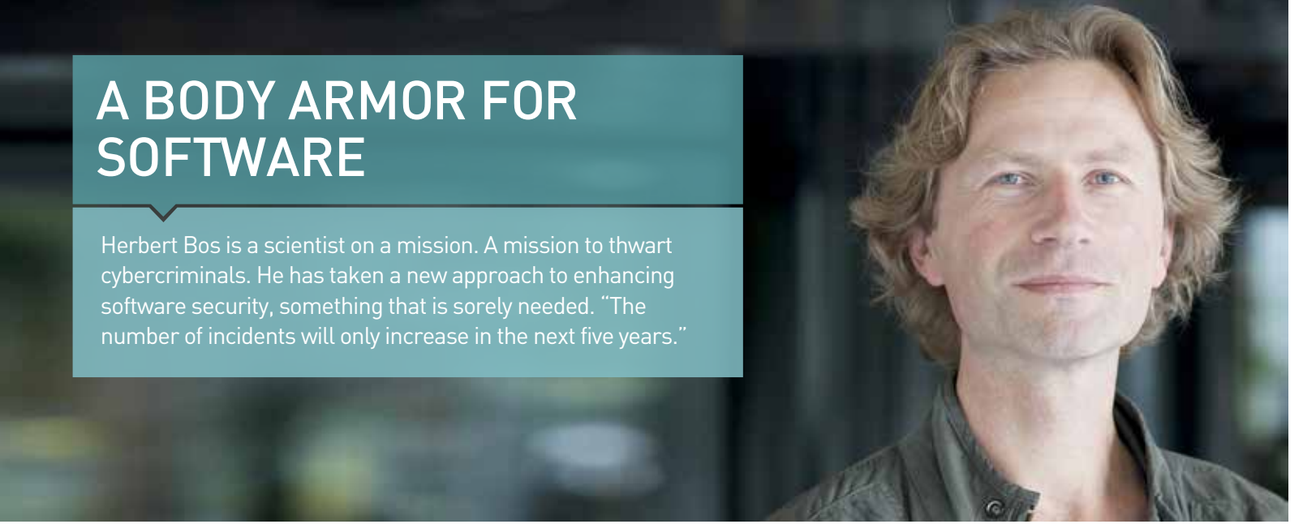

A BODY ARMOR FOR SOFTWARE

Herbert Bos is a scientist on a mission. A mission to thwart cybercriminals. He has taken a new approach to enhancing software security, something that is sorely needed. "The number of incidents will only increase in the next five years."

By Anita Mussche

"I was walking from the railway station to the VU campus, deep in thought about a problem a colleague was having. Then it struck me: I needed to view the problem from a totally different angle." A new method for securing computer programs against cybercrime was born, to help prevent attacks such as the recent hacks on KPN, LinkedIn, banks and governments."

> "Just another meddlesome busybody," you could hear them thinking

Herbert Bos, Professor of Systems and Network Security, is developing systems to protect software against cyberthieves and other criminals. People are finally starting to appreciate the urgency of the situation. "In the past, when I tried to discuss network security with politicians and policy makers they would get irritated. "Just another meddlesome busybody," you could hear them thinking. They're still irritated, but now it's because things aren't moving fast enough for them."

WORLD CLASS

After receiving his PhD from the University of Cambridge, Bos joined the Computer Systems research group at VU University Amsterdam in 2004. He was really able to flourish here. "We're among the top institutes in the world when it comes to building secure computer systems. There are universities in the United States that, across all disciplines of computer science, are better than we are, but we are one of a handful of top universities in Europe in this field."
Following his flash of insight on his way to the campus, Bos received 1.3m euros in the form of a prestigious ERC Starting Grant from the EU. He used these funds to start a major study into reverse engineering. In order to make software programs more secure, you have to know how they work. You only find this in the source code. But software developers tend to keep their source code secret, since this gives them a competitive advantage. Source code can also get lost.. Programs are sometimes used for thirty years or more, and there is a real risk that the company no longer has the source code or even that the company has gone belly-up.

HOLY GRAIL

Normally, securing programs means fiddling with the source code, but now the source code is no longer accessible. "This is a problem that has transfixed researchers for decades. Solving it would be like finding the Holy Grail for us," muses Bos. "Previously, researchers have attempted to use pattern identification on the binary stew of ones and zeros that constitues a program to recover the source code of the program."
Bos' strategy involves a completely different approach. He does not bother with the ones and zeros. Rather, he looks at how the program uses information. The more you know about the information, the more you know about how the program, in other words the source code, works. Bos gives an example: "Imagine a personnel file. It consists of fields such as age, salary, address. The program accesses all fields individually. The contents of one field may resemble a word, perhaps the name of the employee. Another field may contain a number... the salary perhaps, to which amounts are added or subtracted. A word is a different kind of data than a number. This means you extract semantic information from the program." All of this information can gradually lead researchers to the source code.
Nevertheless, Bos has little hope that you can create a completely secure computer system, even if you start from scratch. "The systems have become far too complex for that. And starting from scratch is simply not an option. There is still a lot of old software in use in traffic lights, lift systems, railway installations. System security is only as strong as its weakest link. This is why we want to make old software more secure. In fact, we're trying to stitch up a bulletproof vest around that old, vulnerable software."

> "The sheer complexity of today's computer systems is a surefire guarantee for security breaches"

FOCUSED ON SALES

You would think that software companies such as Microsoft or Apple would secure their own programs, but they are focused far more on sales than on investing in expensive security. "Companies often have a very lax attitude," states Bos resolutely. "On the other hand, it is very difficult to secure computer systems effectively. The sheer complexity of today's computer systems is a surefire guarantee for security breaches. They have become behemoths that can no longer be tamed."
Actively hacking a program is sometimes the most feasible way to discover the weak spots, says Bos. This gives them more insight into the methods of criminal hackers. Once you know where the weak links are, you can do something about them.
Bos loves the hackers' spirit. "Seeing how far you can get, it's a real kick. Hackers are very smart and creative people. At school we used to hack computer games so we wouldn't have to buy them. Outrageous!" he chuckles. Now he teaches his students the craft of hacking. "They are following in the footsteps of super-hacker Kevin Mitnick, who hacked the San Diego Super Computer Center. We've recreated that system in our lab, and students can now go at it like latter-day Kevin Mitnicks." He also encourages his students to participate in international hacking competitions, and they've even formed a regular team.

> "We're going to be facing an enormous shortage of computer scientists"

WARNING

Bos finds it not only fun but also very important to properly educate people, not least because society has a great need for people who know about computer security. "The number of incidents will only increase in the next five years. We're going to be facing an enormous shortage of computer scientists." Bos is inundated with calls from companies looking for trainees or recent graduates.
His teaching is really in the spotlight. The activities of Anonymous, along with other influences, have served to change the nerdy image of computer science as a discipline, he notes. He himself made a deliberate choice for science rather than for business. "I think it's important to do something for society. I see it as our responsibility to issue a warning if things are not properly secured. In the end, citizens will suffer if their private data are breached, or if hackers flood an area with sewage as happened in Australia."
This social component is very important to Bos, as evidenced by his membership in the Securely Connected Innovation Platform and his co-authorship of the National Cyber Security Research Agenda.
Others will be able to conduct further research using the expertise he is amassing. "This matters in society. If you know how a virus attacks a cell, then you can work on developing a suitable antiviral agent. If you know how a virus invades software, then measures can be taken to prevent such breaches."
Bos prefers to stick with science, his great passion. "I am fascinated by the scientific method. I can share that fascination through my teaching and research. These days I still work every evening, but no longer until 4am as in the past." Yet he still finds time for other activities such as sailing, drawing and running. "How do I do it? I sleep very little ... and I have no TV, which saves a lot of time."

> "I sleep very little ... and I have no TV, which saves a lot of time"

MORTIFIED

Besides an impressive number of publications in leading journals, Bos has also supervised quite a few highly successful PhD students. "It's amazing to see how they execute their doctoral research and complete their PhDs. I'm so grateful that I can be part of it." As a professor he does miss engaging in work that requires a bit of elbow grease. "What I enjoy most is working on an interesting problem with a PhD student. We have some very clever young men and women in the group, and it's just great to work with them. They sometimes come up with ideas that are nothing short of genius, things that make you think 'I never would have thought of that on my own.' Awesome. Sometimes I also think: this student has enormous potential and is really going places. As a professor you spend a great deal of time in meetings, supervising students and coordinating activities. If you're not careful, all your research time will evaporate, which sounds like an absolute nightmare. What would really mortify me? That the day will come that I'll be speaking with a PhD student and not understand what he's talking about. But I haven't reached that stage yet, thank goodness!"

CRASH IN TIME

The internet is the cyberburglar's crowbar. Computers can be hijacked, for example by bombarding them with overwhelming amounts of information over the internet, causing a buffer overflow. Your web browser reserves a bit of program memory for loading web pages. If the browser does not check in advance if there is enough space for the incoming information, then other parts of the memory will be overwritten. This could include parts of the memory that hold access rights to certain information. This can leave the computer wide-open for attack.
Bos and his team have developed a new technique, Body Armor, which ensures that a program crashes before it can be hijacked. The program first identifies all buffers in the browser and analyses all instructions that are directed at the buffers. They circumvent the problematic source code by focusing on something else: the machine code. This code consists of very basic instructions that control the computer's processor. This code is also largely unknown, but Bos does know about certain lines of code that are specifically devoted to instructing the processor to write data to the browser's buffer. The researchers adjust these instructions so that any attempt to cause a buffer overflow will be detected and the program will close.