Silver Bullet Talks with Bart Preneel

Gary McGraw | Cigital

Hear the full podcast at www.computer.org/silverbullet. Show links, notes, and an online discussion can be found at www.cigital.com/silverbullet.

Bart Preneel is a professor at the University of Leuven (KU Leuven), Belgium, which was formed in 1425. He's published more than 300 articles and has participated in more than 40 research projects sponsored by the European Commission. His main research interests are cryptology and information security. Bart has lectured all over the world in 40 different countries.

What's it like to be part of one of the oldest universities on Earth?

It's a privilege and an honor to be here. We have an engineering department that's only a bit more than 150 years old, but we do have faculties of law and theology that actually go back to the 15th century.

Do you see differences in general approaches including pedagogy between the EU and the US?

I think there's a very big difference in the kind of research being done. The US is very strong in systems research in security. In Europe, I think we are stronger in formal methods—more abstract stuff in computer science. In my favorite area, cryptography, the work in Europe is much more applied. There are many more people who build concrete systems, work on cryptanalysis, for example, and develop secure embedded hardware and software. This may go back to a tradition where it was hard to get funding in the US for crypto research, especially cryptanalysis.

Do you think engineering in Europe is stronger because it's more mathematically based?

I think many computer science departments grew out of mathematics departments, so this may explain the fact that they had a bigger inclination for more theoretical work and formal methods. There was also a tradition of leaving professors alone and not forcing them to work with industry, which has now changed.

The interaction with Silicon Valley certainly changed the face of computer science in the US.

And there are European copycats. The University of Cambridge has many spin-offs. Even [KU Leuven] is proud to be very highly ranked with more than 100 spinoffs and a close interaction between industry and university.

It's important to have some interaction with industry so you know what applied systems are going to look like. But I also think it can go too far, for example, if the curriculum is dictated by certifications for system administration of a certain database. Does Europe have that pressure like the States do?

There is more autonomy in education here. The education program changes very slowly. There needs to be consensus that goes up to all levels of universities, so sometimes it's even too slow. But I don't think there's much influence from industries on the exact program that's being taught. We encourage internships and collaboration with industry, but with the core curriculum we try to stick to foundations. The idea is that people will pick up the applied stuff in industry.

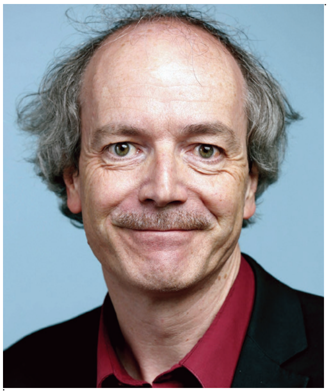
You've lectured in 40 different countries. How seriously is the notion of

1540-7993/15/$31.00 © 2015 IEEE

building security in taken in those different countries?

There's a very big difference in culture, but I would say there's also a very big difference over time. I think the country where people were most behind was Cuba. Interestingly, people in master's programs were writing software that was installed through the Venezuelan government. I found out this was medical software and these people had no clue about cryptography. This topic was kind of forbidden in the university. I was one of the first people to teach them crypto.

In general, Japan and Korea are very advanced. China is catching up very quickly—the awareness and investments there are massive. There were research groups I visited six or seven years ago that had a handful of people and now plan to grow within the next year to 500. Security culture is being developed everywhere. Cybersecurity is a hot topic and I think governments are responding to this.



About Bart Preneel

Bart Preneel is the head of the COSIC (Computer Security and Industrial Cryptography) research group and a professor in the Electrical Engineering Department at Leuven University in Belgium. His research focuses on cryptography, information and system security, and privacy. He has been a visiting professor at universities in Denmark, Austria, Norway, Germany, and Belgium. Preneel has authored and coauthored more than 300 scientific publications and has served as president of the International Association for Cryptologic Research and as a member of the editorial boards of the *Journal of Cryptology*, *IEEE Transactions on Information Forensics and Security*, and *Journal of Computer Security*. He's a member of the Academia Europaea.

Tell us about the major research projects in your research group, COSIC [Computer Security and Industrial Cryptography].

We now have 65 people, and I have four colleague professors, so there are many things happening. Many people are working on CAESAR [Competition for Authenticated Encryption: Security, Applicability, and Robustness], which is a smaller informal competition about authenticated encryption. Cryptographers know from the 1980s that you never want encryption alone—you always want encryption and data authentication. But somehow, we never had a good construction and applied those things separately. So, when security protocols were designed, we had a separate solution with a MAC and an encryption mechanism.

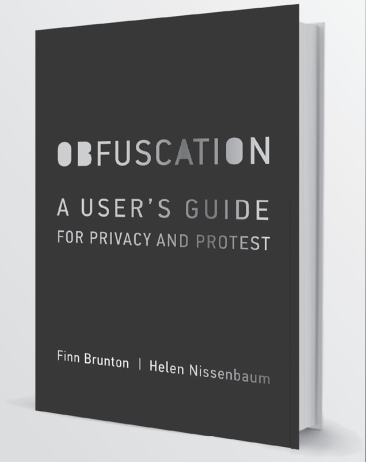
About 15 years ago, some better solutions finally emerged, but it was a bit too late and several were patent encumbered, so there were some problems. What we're using today is actually suboptimal—it has certain performance and robustness problems. So the idea was to start an open competition where teams submitted entries—there were more than 60 schemes and now it's like the Olympics of cryptography. The battle is trying to break schemes and evaluate their performance—this is a very exciting research topic on which several of our team members are working.

I'm very excited about working with our computer science group on better, more secure systems. We have protected modules where we combine crypto with software security methods relying on program counter–based access control. No other process on the machine can read the data or the code, and you have certain guarantees about the code. This is all achieved with a very small overhead. This is low-cost crypto with some very simple software security mechanisms. Together, those can give you some interesting assurances.

You've also spoken about what has changed about applied cryptography in the post-[Edward] Snowden world. What do you think the implications of the Snowden revelations are for crypto?

In some sense, Snowden didn't tell us great secrets. The NSA has been coming to our conferences since the very beginning. I think we were all surprised by the level of sophistication and the scale and nature of some of the things they do. I think we had the image of them being passive listeners. But the image that comes from the Snowden documents is that they are active hackers. It's not only hacking the bad guys—they hack anybody between them and a potential target. So even if you are a system administrator in a telecommunications company, you can be hacked because the company may have data streams that interest the NSA. That's definitely changed our look.

In cryptography, we use the Dolev-Yao model named after a famous paper from the early '80s, which more or less says that a network is taken over by the adversary. We never thought this would actually happen, but I think what we see in the Snowden documents is a picture where, indeed, the NSA owns a network. This kind of attack was imaginable, but the fact that it would actually be deployed and used on a large scale surprised us. I think we need to be much more careful about deployment and our schemes.



What are the implications for system design now?

In crypto, we teach our students to protect secrets—authentication—by protecting a key. But what we've now learned is that there is something called a security letter, which says "give me your key; you can't talk about it or else you'll go to jail." Of course, we don't know about those letters, but we do see some people who actually decide to shut down their businesses. We can deduce that they [received these] letters. If you shift all your secrets to a single key, you're also taking the risk that an agency will come get this key.

We should use techniques that were developed in the '80s and '90s—distribute your secrets over multiple keys and make sure they're under control of multiple independent entities. It becomes much harder to get control of the key. I think putting everything on one key is a big mistake—at least for those sophisticated environments.

It's also about open implementations. We have discovered many things, but in the end if you have a closed source implementation, either a hardware or software module, and if you see what your opponent is prepared to do—what kind of risk they're prepared to take—you should look with even more distrust at anything that is closed source or a closed hardware box. The probability of a back door is so large that you almost have to assume it's there. So I think it actually pushes us. For our security implementation, we should have open source. Of course, Heartbleed proved it's not enough—we also need strong governance for open source.

That's one of the challenges with open source—the economics don't really support the security engineering required to get that stuff right.

What we often do in security is ignore problems—we claim they're not there. We now have the problem in front of us. I'm not a big fan of asking for money from the government, but even before Heartbleed, I spoke in public and said there should be more funding for large-scale code reviews. If the big corporations don't do it, I think the government should intervene and make funds available for reviews of all this code base.

I put the idea forward in the European Parliament, but traction there doesn't happen quickly.

Tell us about the *Journal of Craptology*, which sounds very fun.

I got involved with this at the very beginning. It was inspired in part by the rump sessions. At crypto conferences, they always have an evening session with impromptu talks. About 10 percent of the talks used to be incredibly funny because many people in the crypto community have a good sense of humor. The idea was, why not write those stories down so they can be more widely read? This journal seems to do quite well—it doesn't appear very regularly, but the articles are very funny depending on your sense of humor. I think it has a great future ahead. The only thing I regret is when I review a really bad paper, I'm always tempted to write, "This paper would be great in the *Journal of Craptology*," but I don't want to insult the authors, so I've been able to refrain from doing that.

The Silver Bullet Podcast with Gary McGraw is cosponsored by Cigital and this magazine and is syndicated by SearchSecurity.

Gary McGraw is Cigital's chief technology officer. McGraw received a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him at gem@cigital.com.